Implementing Multicast Routing on Cisco IOS XR Software

**Multicast routing** is a bandwidth-conserving technology that reduces traffic by simultaneously delivering a single stream of information to potentially thousands of corporate recipients and homes. Applications that take advantage of multicast routing include video conferencing, corporate communications, distance learning, and distribution of software, stock quotes, and news.

This document assumes that you are familiar with IPv4 and IPv6 multicast routing configuration tasks and concepts for Cisco IOS XR software.

Multicast routing allows a host to send packets to a subset of all hosts as a group transmission rather than to a single host, as in unicast transmission, or to all hosts, as in broadcast transmission. The subset of hosts is known as **group members** and are identified by a single multicast group address that falls under the IP Class D address range from 224.0.0.0 through 239.255.255.255.

For detailed conceptual information about multicast routing and complete descriptions of the multicast routing commands listed in this module, you can refer to the “Related Documents” section on page MCC-108. To locate documentation for other commands that might appear in the course of executing a configuration task, search online in the Cisco IOS XR Software master command index.

### Feature History for Configuring Multicast Routing on the Cisco CRS Router Software

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 2.0</td>
<td>This feature was introduced on the Cisco CRS.</td>
</tr>
<tr>
<td>Release 3.2</td>
<td>Support was added for the IPv6 routing protocol on the Cisco CRS and for the bootstrap router (BSR) feature.</td>
</tr>
<tr>
<td>Release 3.5.0</td>
<td>Multicast VVPN4 was supported.</td>
</tr>
<tr>
<td>Release 3.7.0</td>
<td>The following new features or functionality were added:</td>
</tr>
<tr>
<td></td>
<td>• Support was added for multihop routing within a default VRF table.</td>
</tr>
<tr>
<td></td>
<td>• A new configuration procedure was added for calculating rate per route.</td>
</tr>
<tr>
<td>Release 3.9.0</td>
<td>Support was added for the following features:</td>
</tr>
<tr>
<td></td>
<td>• Multicast-only fast reroutes (MoFRR) .</td>
</tr>
<tr>
<td></td>
<td>• Point-to-multipoint MPLS label-switched multicast routing.</td>
</tr>
<tr>
<td>Release 4.0</td>
<td>Support for Auto-RP Lite and MVPN Hub and Spoke Topology were added.</td>
</tr>
</tbody>
</table>
Contents

- Prerequisites for Implementing Multicast Routing, page MCC-2
- Information About Implementing Multicast Routing, page MCC-2
- How to Implement Multicast Routing, page MCC-25
- Configuration Examples for Implementing Multicast Routing on Cisco IOS XR Software, page MCC-70
- Additional References, page MCC-108

Prerequisites for Implementing Multicast Routing

- You must install and activate a Package Installation Envelope (PIE) for the multicast routing software. For detailed information about optional PIE installation, see Cisco IOS XR Getting Started Guide for the Cisco CRS Router.
- To perform these configuration tasks, your Cisco IOS XR software system administrator must assign you to a user group associated with a task group that includes the corresponding command task IDs. All command task IDs are listed in individual command references and in the Cisco IOS XR Task ID Reference Guide.
  
  If you need assistance with your task group assignment, contact your system administrator. For detailed information about user groups and task IDs, see the Configuring AAA Services on Cisco IOS XR Software module of Cisco IOS XR Software System Security Configuration Guide.
- You must be familiar with IPv4 and IPv6 multicast routing configuration tasks and concepts.
- Unicast routing must be operational.

Information About Implementing Multicast Routing

- Key Protocols and Features Supported in the Cisco IOS XR Software Multicast Routing Implementation, page MCC-3
- Multicast Routing Functional Overview, page MCC-4
- Internet Group Management Protocol and Multicast Listener Discovery, page MCC-5
- Protocol Independent Multicast, page MCC-7
- PIM Shared Tree and Source Tree (Shortest Path Tree), page MCC-8
- Multicast-Intact, page MCC-9
- Designated Routers, page MCC-10
- Rendezvous Points, page MCC-11
- Auto-RP, page MCC-12
- PIM Bootstrap Router, page MCC-12
- Reverse-Path Forwarding, page MCC-13
- Multicast VPN, page MCC-13
- Multitopology Routing, page MCC-16
Key Protocols and Features Supported in the Cisco IOS XR Software Multicast Routing Implementation

Table 1 lists the supported features for IPv4 and IPv6 multicast routing in Cisco IOS XR Software.

<table>
<thead>
<tr>
<th>Feature</th>
<th>IPv4 Support</th>
<th>IPv6 Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic host registration</td>
<td>Yes (IGMP v1/2/3)</td>
<td>Yes (MLD v1/2)</td>
</tr>
<tr>
<td>Explicit tracking of hosts, groups,</td>
<td>Yes (IGMP v3)</td>
<td>Yes (MLD v2)</td>
</tr>
<tr>
<td>and channels</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PIM-SM1</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>PIM-SSM2</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>PIM-Bidir3</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Auto-RP</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Multicast VPN</td>
<td>Yes</td>
<td>Yes4</td>
</tr>
<tr>
<td>BSR3</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>MSDP6</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>BGP7</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Multicast NSF8</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>OOR handling9</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

1. Protocol Independent Multicast in sparse mode
2. Protocol Independent Multicast in Source-Specific Multicast
3. Protocol Independent Multicast Bidirectional
4. IPv6 support on Cisco XR 12000 Series Router only
5. PIM bootstrap router
6. Multicast Source Discovery Protocol
7. Multiprotocol Border Gateway Protocol
8. Nonstop forwarding
9. Out of resource
Multicast Routing Functional Overview

Traditional IP communication allows a host to send packets to a single host (unicast transmission) or to all hosts (broadcast transmission). Multicast provides a third scheme, allowing a host to send a single data stream to a subset of all hosts (group transmission) at about the same time. IP hosts are known as group members.

Packets delivered to group members are identified by a single multicast group address. Multicast packets are delivered to a group using best-effort reliability, just like IP unicast packets.

The multicast environment consists of senders and receivers. Any host, regardless of whether it is a member of a group, can send to a group. However, only the members of a group receive the message.

A multicast address is chosen for the receivers in a multicast group. Senders use that group address as the destination address of a datagram to reach all members of the group.

Membership in a multicast group is dynamic; hosts can join and leave at any time. There is no restriction on the location or number of members in a multicast group. A host can be a member of more than one multicast group at a time.

How active a multicast group is and what members it has can vary from group to group and from time to time. A multicast group can be active for a long time, or it may be very short-lived. Membership in a group can change constantly. A group that has members may have no activity.

Routers use the Internet Group Management Protocol (IGMP) (IPv4) and Multicast Listener Discovery (MLD) (IPv6) to learn whether members of a group are present on their directly attached subnets. Hosts join multicast groups by sending IGMP or MLD report messages.

Many multimedia applications involve multiple participants. Multicast is naturally suitable for this communication paradigm.

Cisco IOS XR Multicast Routing Implementation

Cisco IOS XR Software supports the following protocols to implement multicast routing:

- IGMP and MLD are used (depending on the IP protocol) between hosts on a LAN and the routers on that LAN to track the multicast groups of which hosts are members.
- Protocol Independent Multicast in sparse mode (PIM-SM) is used between routers so that they can track which multicast packets to forward to each other and to their directly connected LANs.
- Protocol Independent Multicast in Source-Specific Multicast (PIM-SSM) is similar to PIM-SM with the additional ability to report interest in receiving packets from specific source addresses (or from all but the specific source addresses), to an IP multicast address.
- PIM-SSM is made possible by IGMPv3 and MLDv2. Hosts can now indicate interest in specific sources using IGMPv3 and MLDv2. SSM does not require a rendezvous point (RP) to operate.

Figure 1 shows IGMP/MLD and PIM-SM operating in a multicast environment.
Internet Group Management Protocol and Multicast Listener Discovery

Cisco IOS XR software provides support for Internet Group Management Protocol (IGMP) over IPv4 and Multicast Listener Discovery (MLD) over IPv6.

IGMP and MLD provide a means for hosts to indicate which multicast traffic they are interested in and for routers to control and limit the flow of multicast traffic throughout the network. Routers build state by means of IGMP and MLD messages; that is, router queries and host reports.

A set of queries and hosts that receive multicast data streams from the same source is called a multicast group. Hosts use IGMP and MLD messages to join and leave multicast groups.

**Note**

IGMP messages use group addresses, which are Class D IP addresses. The high-order four bits of a Class D address are 1110. Host group addresses can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is guaranteed not to be assigned to any group. The address 224.0.0.1 is assigned to all systems on a subnet. The address 224.0.0.2 is assigned to all routers on a subnet.

**IGMP and MLD Versions**

The following points describe IGMP versions 1, 2, and 3:

- IGMP Version 1 provides for the basic query-response mechanism that allows the multicast router to determine which multicast groups are active and for other processes that enable hosts to join and leave a multicast group.
- IGMP Version 2 extends IGMP allowing such features as the IGMP query timeout and the maximum query-response time. See RFC 2236.
MLDv1 provides the same functionality (under IPv6) as IGMP Version 2.

- IGMP Version 3 permits joins and leaves for certain source and group pairs instead of requesting traffic from all sources in the multicast group.

MLDv2 provides the same functionality (under IPv6) as IGMP Version 3.

**IGMP Routing Example**

Figure 2 illustrates two sources, 10.0.0.1 and 10.0.1.1, that are multicasting to group 239.1.1.1. The receiver wants to receive traffic addressed to group 239.1.1.1 from source 10.0.0.1 but not from source 10.0.1.1. The host must send an IGMPv3 message containing a list of sources and groups (S, G) that it wants to join and a list of sources and groups (S, G) that it wants to leave. Router C can now use this information to prune traffic from Source 10.0.0.1 so that only Source 10.0.0.1 traffic is being delivered to Router C.

**Figure 2** IGMPv3 Signaling

When configuring IGMP, ensure that all systems on the subnet support the same IGMP version. The router does not automatically detect Version 1 systems. Configure the router for Version 2 if your hosts do not support Version 3.
Protocol Independent Multicast

Protocol Independent Multicast (PIM) is a routing protocol designed to send and receive multicast routing updates. Proper operation of multicast depends on knowing the unicast paths towards a source or an RP. PIM relies on unicast routing protocols to derive this reverse-path forwarding (RPF) information. As the name PIM implies, it functions independently of the unicast protocols being used. PIM relies on the Routing Information Base (RIB) for RPF information. If the multicast subsequent address family identifier (SAFI) is configured for Border Gateway Protocol (BGP), or if multicast intact is configured, a separate multicast unicast RIB is created and populated with the BGP multicast SAFI routes, the intact information, and any IGP information in the unicast RIB. Otherwise, PIM gets information directly from the unicast SAFI RIB. Both multicast unicast and unicast databases are outside of the scope of PIM.


Note
Cisco IOS XR Software supports PIM-SM, PIM-SSM, PIM Bidir, and PIM Version 2 only. PIM Version 1 hello messages that arrive from neighbors are rejected.

PIM-Sparse Mode

Typically, PIM in sparse mode (PIM-SM) operation is used in a multicast network when relatively few routers are involved in each multicast. Routers do not forward multicast packets for a group, unless there is an explicit request for traffic. Requests are accomplished using PIM join messages, which are sent hop by hop toward the root node of the tree. The root node of a tree in PIM-SM is the rendezvous point (RP) in the case of a shared tree or the first-hop router that is directly connected to the multicast source in the case of a shortest path tree (SPT). The RP keeps track of multicast groups, and the sources that send multicast packets are registered with the RP by the first-hop router of the source.

As a PIM join travels up the tree, routers along the path set up the multicast forwarding state so that the requested multicast traffic is forwarded back down the tree. When multicast traffic is no longer needed, a router sends a PIM prune message up the tree toward the root node to prune (or remove) the unnecessary traffic. As this PIM prune travels hop by hop up the tree, each router updates its forwarding state appropriately. Ultimately, the forwarding state associated with a multicast group or source is removed. Additionally, if prunes are not explicitly sent, the PIM state will timeout and be removed in the absence of any further join messages.

PIM-SM is the best choice for multicast networks that have potential members at the end of WAN links.

PIM-Source Specific Multicast

In many multicast deployments where the source is known, protocol-independent multicast-source-specific multicast (PIM-SSM) mapping is the obvious multicast routing protocol choice to use because of its simplicity. Typical multicast deployments that benefit from PIM-SSM consist of entertainment-type solutions like the ETTH space, or financial deployments that completely rely on static forwarding.

PIM-SSM is derived from PIM-SM. However, whereas PIM-SM allows for the data transmission of all sources sending to a particular group in response to PIM join messages, the SSM feature forwards traffic to receivers only from those sources that the receivers have explicitly joined. Because PIM joins and
prunes are sent directly towards the source sending traffic, an RP and shared trees are unnecessary and are disallowed. SSM is used to optimize bandwidth utilization and deny unwanted Internet broadcast traffic. The source is provided by interested receivers through IGMPv3 membership reports.

In SSM, delivery of datagrams is based on (S,G) channels. Traffic for one (S,G) channel consists of datagrams with an IP unicast source address S and the multicast group address G as the IP destination address. Systems receive traffic by becoming members of the (S,G) channel. Signaling is not required, but receivers must subscribe or unsubscribe to (S,G) channels to receive or not receive traffic from specific sources. Channel subscription signaling uses IGMP to include mode membership reports, which are supported only in Version 3 of IGMP (IGMPv3).

To run SSM with IGMPv3, SSM must be supported on the multicast router, the host where the application is running, and the application itself. Cisco IOS XR Software allows SSM configuration for an arbitrary subset of the IP multicast address range 224.0.0.0 through 239.255.255.255. When an SSM range is defined, existing IP multicast receiver applications do not receive any traffic when they try to use addresses in the SSM range, unless the application is modified to use explicit (S,G) channel subscription.

**PIM Shared Tree and Source Tree (Shortest Path Tree)**

In PIM-SM, the rendezvous point (RP) is used to bridge sources sending data to a particular group with receivers sending joins for that group. In the initial setup of state, interested receivers receive data from senders to the group across a single data distribution tree rooted at the RP. This type of distribution tree is called a shared tree or rendezvous point tree (RPT) as illustrated in Figure 3. Data from senders is delivered to the RP for distribution to group members joined to the shared tree.

![Figure 3 Shared Tree and Source Tree (Shortest Path Tree)](image)

Unless the `spt-threshold infinity` command is configured, this initial state gives way as soon as traffic is received on the leaf routers (designated router closest to the host receivers). When the leaf router receives traffic from the RP on the RPT, the router initiates a switch to a data distribution tree rooted at
the source sending traffic. This type of distribution tree is called a **shortest path tree** or **source tree**. By default, the Cisco IOS XR software switches to a source tree when it receives the first data packet from a source.

The following process describes the move from shared tree to source tree in more detail:

1. Receiver joins a group; leaf Router C sends a join message toward RP.
2. RP puts link to Router C in its outgoing interface list.
3. Source sends data; Router A encapsulates data in Register and sends it to RP.
4. RP forwards data down the shared tree to Router C and sends a join message toward Source. At this point, data may arrive twice at the RP, once encapsulated and once natively.
5. When data arrives natively (unencapsulated) at RP, RP sends a register-stop message to Router A.
6. By default, receipt of the first data packet prompts Router C to send a join message toward Source.
7. When Router C receives data on (S,G), it sends a prune message for Source up the shared tree.
8. RP deletes the link to Router C from outgoing interface of (S,G). RP triggers a prune message toward Source.

Join and prune messages are sent for sources and RPs. They are sent hop by hop and are processed by each PIM router along the path to the source or RP. Register and register-stop messages are not sent hop by hop. They are exchanged using direct unicast communication between the designated router that is directly connected to a source and the RP for the group.

**Tip**

The `spt-threshold infinity` command lets you configure the router so that it never switches to the shortest path tree (SPT).

## Multicast-Intact

The multicast-intact feature provides the ability to run multicast routing (PIM) when Interior Gateway Protocol (IGP) shortcuts are configured and active on the router. Both Open Shortest Path First, version 2 (OSPFv2), and Intermediate System-to-Intermediate System (IS-IS) support the multicast-intact feature. Multiprotocol Label Switching Traffic Engineering (MPLS-TE) and IP multicast coexistence is supported in Cisco IOS XR Software by using the `mpls traffic-eng multicast-intact` IS-IS or OSPF router command. See Cisco IOS XR Routing Configuration Guide for the Cisco CRS-1 Router for information on configuring multicast intact using IS-IS and OSPF commands.

You can enable multicast-intact in the IGP when multicast routing protocols (PIM) are configured and IGP shortcuts are configured on the router. IGP shortcuts are MPLS tunnels that are exposed to IGP. The IGPs route the IP traffic over these tunnels to destinations that are downstream from the egress router of the tunnel (from an SPF perspective). PIM cannot use IGP shortcuts for propagating PIM joins because reverse path forwarding (RPF) cannot work across a unidirectional tunnel.

When you enable multicast-intact on an IGP, the IGP publishes a parallel or alternate set of equal-cost next-hops for use by PIM. These next-hops are called **mcast-intact next-hops**. The mcast-intact next-hops have the following attributes:

- They are guaranteed not to contain any IGP shortcuts.
- They are not used for unicast routing but are used only by PIM to look up an IPv4 next hop to a PIM source.
- They are not published to the Forwarding Information Base (FIB).
When multicast-intact is enabled on an IGP, all IPv4 destinations that were learned through link-state advertisements are published with a set equal-cost mcast-intact next-hops to the RIB. This attribute applies even when the native next-hops have no IGP shortcuts.

In IS-IS, the max-paths limit is applied by counting both the native and mcast-intact next-hops together. (In OSPFv2, the behavior is slightly different.)

### Designated Routers

Cisco routers use PIM-SM to forward multicast traffic and follow an election process to select a designated router (DR) when there is more than one router on a LAN segment.

The designated router is responsible for sending PIM register and PIM join and prune messages toward the RP to inform it about host group membership.

If there are multiple PIM-SM routers on a LAN, a designated router must be elected to avoid duplicating multicast traffic for connected hosts. The PIM router with the highest IP address becomes the DR for the LAN unless you choose to force the DR election by use of the `dr-priority` command. The DR priority option allows you to specify the DR priority of each router on the LAN segment (default priority = 1) so that the router with the highest priority is elected as the DR. If all routers on the LAN segment have the same priority, the highest IP address is again used as the tiebreaker.

*Figure 4* illustrates what happens on a multiaccess segment. Router A (10.0.0.253) and Router B (10.0.0.251) are connected to a common multiaccess Ethernet segment with Host A (10.0.0.1) as an active receiver for Group A. As the Explicit Join model is used, only Router A, operating as the DR, sends joins to the RP to construct the shared tree for Group A. If Router B were also permitted to send (*, G) joins to the RP, parallel paths would be created and Host A would receive duplicate multicast traffic. When Host A begins to source multicast traffic to the group, the DR's responsibility is to send register messages to the RP. Again, if both routers were assigned the responsibility, the RP would receive duplicate multicast packets.

If the DR fails, the PIM-SM provides a way to detect the failure of Router A and to elect a failover DR. If the DR (Router A) were to become inoperable, Router B would detect this situation when its neighbor adjacency with Router A timed out. Because Router B has been hearing IGMP membership reports from Host A, it already has IGMP state for Group A on this interface and immediately sends a join to the RP when it becomes the new DR. This step reestablishes traffic flow down a new branch of the shared tree using Router B. Additionally, if Host A were sourcing traffic, Router B would initiate a new register process immediately after receiving the next multicast packet from Host A. This action would trigger the RP to join the SPT to Host A, using a new branch through Router B.

---

**Tip**

Two PIM routers are neighbors if there is a direct connection between them. To display your PIM neighbors, use the `show pim neighbor` command in EXEC mode.
Rendezvous Points

When PIM is configured in sparse mode, you must choose one or more routers to operate as a rendezvous point (RP). A rendezvous point is a single common root placed at a chosen point of a shared distribution tree, as illustrated in Figure 3. A rendezvous point can be either configured statically in each box or learned through a dynamic mechanism.

PIM DRs forward data from directly connected multicast sources to the rendezvous point for distribution down the shared tree. Data is forwarded to the rendezvous point in one of two ways:

- Encapsulated in register packets and unicast directly to the rendezvous point by the first-hop router operating as the DR.
- Multicast forwarded by the RPF forwarding algorithm, described in the “Reverse-Path Forwarding” section on page MCC-13, if the rendezvous point has itself joined the source tree.

The rendezvous point address is used by first-hop routers to send PIM register messages on behalf of a host sending a packet to the group. The rendezvous point address is also used by last-hop routers to send PIM join and prune messages to the rendezvous point to inform it about group membership. You must configure the rendezvous point address on all routers (including the rendezvous point router).

A PIM router can be a rendezvous point for more than one group. Only one rendezvous point address can be used at a time within a PIM domain. The conditions specified by the access list determine for which groups the router is a rendezvous point.
You can either manually configure a PIM router to function as a rendezvous point or allow the rendezvous point to learn group-to-RP mappings automatically by configuring Auto-RP or BSR. (For more information, see the “Auto-RP” section that follows and “PIM Bootstrap Router” section on page MCC-12.)

**Auto-RP**

Automatic route processing (Auto-RP) is a feature that automates the distribution of group-to-RP mappings in a PIM network. This feature has these benefits:

- It is easy to use multiple RPs within a network to serve different group ranges.
- It allows load splitting among different RPs.
- It facilitates the arrangement of RPs according to the location of group participants.
- It avoids inconsistent, manual RP configurations that might cause connectivity problems.

Multiple RPs can be used to serve different group ranges or to serve as hot backups for each other. To ensure that Auto-RP functions, configure routers as candidate RPs so that they can announce their interest in operating as an RP for certain group ranges. Additionally, a router must be designated as an RP-mapping agent that receives the RP-announcement messages from the candidate RPs, and arbitrates conflicts. The RP-mapping agent sends the consistent group-to-RP mappings to all remaining routers. Thus, all routers automatically determine which RP to use for the groups they support.

**Tip**

By default, if a given group address is covered by group-to-RP mappings from both static RP configuration, and is discovered using Auto-RP or PIM BSR, the Auto-RP or PIM BSR range is preferred. To override the default, and use only the RP mapping, use the `rp-address override` keyword.

**Note**

If you configure PIM in sparse mode and do not configure Auto-RP, you must statically configure an RP as described in the “Configuring a Static RP and Allowing Backward Compatibility” section on page MCC-29. When router interfaces are configured in sparse mode, Auto-RP can still be used if all routers are configured with a static RP address for the Auto-RP groups.

**Note**

Auto-RP is not supported on VRF interfaces. Auto-RP Lite allows you to configure auto-RP on the CE router. It allows the PE router that has the VRF interface to relay auto-RP discovery, and announce messages across the core and eventually to the remote CE. Auto-RP is supported in only the IPv4 address family.

**PIM Bootstrap Router**

The PIM bootstrap router (BSR) provides a fault-tolerant, automated RP discovery and distribution mechanism that simplifies the Auto-RP process. This feature is enabled by default allowing routers to dynamically learn the group-to-RP mappings.

PIM uses the BSR to discover and announce RP-set information for each group prefix to all the routers in a PIM domain. This is the same function accomplished by Auto-RP, but the BSR is part of the PIM Version 2 specification. The BSR mechanism interoperates with Auto-RP on Cisco routers.
To avoid a single point of failure, you can configure several candidate BSRs in a PIM domain. A BSR is elected among the candidate BSRs automatically. Candidates use bootstrap messages to discover which BSR has the highest priority. The candidate with the highest priority sends an announcement to all PIM routers in the PIM domain that it is the BSR.

Routers that are configured as candidate RPs unicast to the BSR the group range for which they are responsible. The BSR includes this information in its bootstrap messages and disseminates it to all PIM routers in the domain. Based on this information, all routers are able to map multicast groups to specific RPs. As long as a router is receiving the bootstrap message, it has a current RP map.

Reverse-Path Forwarding

Reverse-path forwarding (RPF) is an algorithm used for forwarding multicast datagrams. It functions as follows:

- If a router receives a datagram on an interface it uses to send unicast packets to the source, the packet has arrived on the RPF interface.
- If the packet arrives on the RPF interface, a router forwards the packet out the interfaces present in the outgoing interface list of a multicast routing table entry.
- If the packet does not arrive on the RPF interface, the packet is silently discarded to prevent loops.

PIM uses both source trees and RP-rooted shared trees to forward datagrams; the RPF check is performed differently for each, as follows:

- If a PIM router has an (S,G) entry present in the multicast routing table (a source-tree state), the router performs the RPF check against the IP address of the source for the multicast packet.
- If a PIM router has no explicit source-tree state, this is considered a shared-tree state. The router performs the RPF check on the address of the RP, which is known when members join the group.

Sparse-mode PIM uses the RPF lookup function to determine where it needs to send joins and prunes. (S,G) joins (which are source-tree states) are sent toward the source. (*,G) joins (which are shared-tree states) are sent toward the RP.

Multicast VPN

To provide Layer 3 multicast services to customers with multiple distributed sites, service providers look for a secure and scalable mechanism to transmit customer multicast traffic across the provider network. Multicast VPN (MVPN) provides such services over a shared service provider backbone, using native multicast technology similar to BGP/MPLS VPN.

MVPN emulates MPLS VPN technology in its adoption of the multicast domain (MD) concept, in which provider edge (PE) routers establish virtual PIM neighbor connections with other PE routers that are connected to the same customer VPN. These PE routers thereby form a secure, virtual multicast domain over the provider network. Multicast traffic is then transmitted across the core network from one site to another, as if the traffic were going through a dedicated provider network.

Separate multicast routing and forwarding tables are maintained for each VPN routing and forwarding (VRF) instance, with traffic being sent through VPN tunnels across the service provider backbone. **Multicast VPN Routing and Forwarding**

Dedicated multicast routing and forwarding tables are created for each VPN to separate traffic in one VPN from traffic in another.
The VPN-specific multicast routing and forwarding database is referred to as **MVRF**. On a PE router, an MVRF is created when multicast is enabled for a VRF. Protocol Independent Multicast (PIM), and Internet Group Management Protocol (IGMP) protocols run in the context of MVRF, and all routes created by an MVRF protocol instance are associated with the corresponding MVRF. In addition to VRFs, which hold VPN-specific protocol states, a PE router always has a global VRF instance, containing all routing and forwarding information for the provider network.

**Multicast Distribution Tree Tunnels**

The multicast distribution tree (MDT) can span multiple customer sites through provider networks, allowing traffic to flow from one source to multiple receivers.

Secure data transmission of multicast packets sent from the customer edge (CE) router at the ingress PE router is achieved by encapsulating the packets in a provider header and transmitting the packets across the core. At the egress PE router, the encapsulated packets are decapsulated and then sent to the CE receiving routers.

Multicast distribution tree (MDT) tunnels are point-to-multipoint. A MDT tunnel interface is an interface that MVRF uses to access the multicast domain. It can be deemed as a passage that connects an MVRF and the global MVRF. Packets sent to an MDT tunnel interface are received by multiple receiving routers. Packets sent to an MDT tunnel interface are encapsulated, and packets received from a MDT tunnel interface are decapsulated.

![Figure 5 Virtual PIM Peer Connection over an MDT Tunnel Interface](image_url)

Encapsulating multicast packets in a provider header allows PE routers to be kept unaware of the packets’ origin—all VPN packets passing through the provider network are viewed as native multicast packets and are routed based on the routing information in the core network. To support MVPN, PE routers only need to support native multicast routing.

MVVPN also supports optimized VPN traffic forwarding for high-bandwidth applications that have sparsely distributed receivers. A dedicated multicast group can be used to encapsulate packets from a specific source, and an optimized MDT can be created to send traffic only to PE routers connected to interested receivers. This is referred to as **data MDT**.

**InterAS Support on Multicast VPN**

The Multicast VPN Inter-AS Support feature enables service providers to provide multicast connectivity to VPN sites that span across multiple autonomous systems. This feature enables Multicast Distribution Trees (MDTs), used for Multicast VPNs (MVVPN), to span multiple autonomous systems.
There are two types of MVPN inter-AS deployment scenarios:

- Single-Provider Inter-AS—A service provider whose internal network consists of multiple autonomous systems.
- Intra-Provider Inter-AS—Multiple service providers that need to coordinate their networks to provide inter-AS support.

To establish a Multicast VPN between two autonomous systems, a MDT-default tunnel must be setup between the two PE routers. The PE routers accomplish this by joining the configured MDT-default group. This MDT-default group is configured on the PE router and is unique for each VPN. The PIM sends the join based on the mode of the groups, which can be PIM SSM, bidir, or sparse mode.

**Benefits of MVPN Inter-AS Support**

The MVPN Inter-AS Support feature provides these benefits to service providers:

- Increased multicast coverage to customers that require multicast to span multiple services providers in an MPLS Layer 3 VPN service.
- The ability to consolidate an existing MVPN service with another MVPN service, as in the case of a company merger or acquisition.

**InterAS Option A**

InterAS Option A is the basic Multicast VPN configuration option. In this option, the PE router partially plays the Autonomous System Border Router (ASBR) role in each Autonomous System (AS). Such a PE router in each AS is directly connected through multiple VRF bearing subinterfaces. MPLS label distribution protocol need not run between these InterAS peering PE routers. However, an IGP or BGP protocol can be used for route distribution under the VRF.

The Option A model assumes direct connectivity between PE routers of different autonomous systems. The PE routers are attached by multiple physical or logical interfaces, each of which is associated with a given VPN (through a VRF instance). Each PE router, therefore, treats the adjacent PE router like a customer edge (CE) router. The standard Layer 3 MPLS VPN mechanisms are used for route redistribution with each autonomous system; that is, the PEs use exterior BGP (eBGP) to distribute unlabeled IPv4 addresses to each other.

**Note**

Option A allows service providers to isolate each autonomous system from the other. This provides better control over routing exchanges and security between the two networks. However, Option A is considered the least scalable of all the inter-AS connectivity options.

**MVPN IPv4 and IPv6 Connectivity**

MVPN IPv4 and IPv6 Connectivity MPVN services occur over IPv4 core networks. IPv6 connectivity is supported between customer sites over an IPv4-only core network with a default VRF. VPN PE routers must interoperate between the two address families, with control and forwarding actions between IPv4-encapsulated MDTs and IPv6 customer routes. In this document, therefore, MVPNv4 refers to the core network, while MVPNv6 refers to IPv6-over-IPv4 functionality.

IPv4 generic routing encapsulation (GRE) multicast distribution trees (MDTs) are supported over the service provider network, while currently, IPv6-encapsulated MDTs are unsupported.
BGP Requirements

PE routers are the only routers that need to be MVPN-aware and able to signal remote PEs with information regarding the MVPN. It is fundamental that all PE routers have a BGP relationship with each other, either directly or through a route reflector, because the PE routers use the BGP peering address information to derive the RPF PE peer within a given VRF.

PIM-SSM MDT tunnels cannot be set up without a configured BGP MDT address-family, because you establish the tunnels, using the BGP connector attribute.

See the Implementing BGP on Cisco IOS XR Software module of the Cisco IOS XR Routing Configuration Guide for information on BGP support for Multicast VPN.

Multitopology Routing

Multitopology routing allows you to manipulate network traffic flow when desirable (for example, to broadcast duplicate video streams) to flow over non-overlapping paths.

At the core of multitopology routing technology is router space infrastructure (RSI). RSI manages the global configuration of routing tables. These tables are hierarchically organized into VRF tables under logical routers. By default, RSI creates tables for unicast and multicast for both IPv4 and IPv6 under the default VRF. Using multitopology routing, you can configure named topologies for the default VRF.

PIM uses a routing policy that supports matching on source or group address to select the topology in which to look up the reverse-path forwarding (RPF) path to the source. If you do not configure a policy, the existing behavior (to select a default table) remains in force.

Currently, IS-IS and PIM routing protocols alone support multitopology-enabled network.

For information on how to configure multitopology routing, see Configuring Multitopology Routing, page MCC-50.

Multicast VPN Extranet Routing

Multicast VPN (MVPN) extranet routing lets service providers distribute IP multicast content from one enterprise site to another across a multicast VRF. In other words, this feature provides capability to seamlessly hop VRF boundaries to distribute multicast content end to end.

Unicast extranet can be achieved simply by configuring matching route targets across VRFs. However, multicast extranet requires such configuration to resolve route lookups across VRFs in addition to the following:

- Maintain multicast topology maps across VRFs.
- Maintain multicast distribution trees to forward traffic across VRFs.

Information About Extranets

An extranet can be viewed as part of an enterprise intranet that is extended to users outside the enterprise. A VPN is used as a way to do business with other enterprises and with customers, such as selling products and maintaining strong business partnerships. An extranet is a VPN that connects to one or more corporate sites to external business partners or suppliers to securely share a designated part of the enterprise’s business information or operations.

MVPN extranet routing can be used to solve such business problems as:
• Inefficient content distribution between enterprises.
• Inefficient content distribution from service providers or content providers to their enterprise VPN customers.

MVPN extranet routing provides support for IPv4 and IPv6 address family.

An extranet network requires the PE routers to pass traffic across VRFs (labeled “P” in Figure 6). Extranet networks can run either IPv4 or IPv6, but the core network always runs only IPv4 active multicast.

Extranet Components

**Figure 6 Components of an Extranet MVPN**

MVRF—Multicast VPN routing and forwarding (VRF) instance. An MVRF is a multicast-enabled VRF. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table. In general, a VRF includes the routing information that defines a customer VPN site that is attached to a provider edge (PE) router.

Source MVRF—An MVRF that can reach the source through a directly connected customer edge (CE) router.

Receiver MVRF—An MVRF to which receivers are connected through one or more CE devices.

Source PE—A PE router that has a multicast source behind a directly connected CE router.

Receiver PE—A PE router that has one or more interested receivers behind a directly connected CE router.

**Information About the Extranet MVPN Routing Topology**

In unicast routing of peer-to-peer VPNs, BGP routing protocol is used to advertise VPN IPv4 and IPv6 customer routes between provider edge (PE) routers. However, in an MVPN extranet peer-to-peer network, PIM RPF is used to determine whether the RPF next hop is in the same or a different VRF and whether that source VRF is local or remote to the PE.
Source MVRF on a Receiver PE Router

To provide extranet MVPN services to enterprise VPN customers by configuring a source MVRF on a receiver PE router, you would complete the following procedure:

- On a receiver PE router that has one or more interested receivers in an extranet site behind a directly connected CE router, configure an MVRF that has the same default MDT group as the site connected to the multicast source.
- On the receiver PE router, configure the same unicast routing policy to import routes from the source MVRF to the receiver MVRF.

If the originating MVRF of the RPF next hop is local (source MVRF at receiver PE router), the join state of the receiver VRFs propagates over the core by using the default multicast distribution tree (MDT) of the source VRF. Figure 7 illustrates the flow of multicast traffic in an extranet MVPN topology where the source MVRF is configured on a receiver PE router (source at receiver MVRF topology). An MVRF is configured for VPN-A and VPN-B on PE2, a receiver PE router. A multicast source behind PE1, the source PE router, is sending out a multicast stream to the MVRF for VPN-A, and there are interested receivers behind PE2, the receiver PE router for VPN-B, and also behind PE3, the receiver PE router for VPN-A. After PE1 receives the packets from the source in the MVRF for VPN-A, it replicates and forwards the packets to PE2 and PE3. The packets received at PE2 in VPN-A are decapsulated and replicated to receivers in VPN-B.

![Figure 7: Source MVRF at the Receiver PE Router](image)

Receiver MVRF on the Source PE Router

To provide extranet MVPN services to enterprise VPN customers by configuring the receiver MVRF on the source PE router, complete the following procedure:

- For each extranet site, you would configure an additional MVRF on the source PE router, which has the same default MDT group as the receiver MVRF, if the MVRF is not already configured on the source PE.
- In the receiver MVRF configuration, you would configure the same unicast routing policy on the source and receiver PE routers to import routes from the source MVRF to the receiver MVRF.

If the originating MVRF of the RPF next-hop is remote (receiver MVRF on the source PE router), the join state of receiver VRFs propagates over the core through the MDT of each receiver.
Figure 8 illustrates the flow of multicast traffic in an extranet MVPN topology where a receiver MVRF is configured on the source PE router. An MVRF is configured for VPN-A and VPN-B on PE1, the source PE router. A multicast source behind PE1 is sending out a multicast stream to the MVRF for VPN-A, and there are interested receivers behind PE2 and PE3, the receiver PE routers for VPN-B and VPN-A, respectively. After PE1 receives the packets from the source in the MVRF for VPN-A, it independently replicates and encapsulates the packets in the MVRF for VPN-A and VPN-B and forwards the packets. After receiving the packets from this source, PE2 and PE3 decapsulate and forward the packets to the respective MVRFs.

For more information, see also Configuring MVPN Extranet Routing, page MCC-52 and Configuring MVPN Extranet Routing: Example, page MCC-85.

RPF Policies in an Extranet

RPF policies can be configured in receiver VRFs to bypass RPF lookup in receiver VRFs and statically propagate join states to specified source VRF. Such policies can be configured to pick a source VRF based on either multicast group range, multicast source range, or RP address.

For more information about configuration of RFP policies in extranets, see Configuring RPL Policies in Receiver VRFs to Propagate Joins to a Source VRF: Example, page MCC-87 and Configuring RPL Policies in Receiver VRFs on Source PE Routers to Propagate Joins to a Source VRF: Example, page MCC-90.

Multicast VPN Hub and Spoke Topology

Hub and spoke topology is an interconnection of two categories of sites — Hub sites and Spoke sites. The routes advertised across sites are such that they achieve connectivity in a restricted hub and spoke fashion. A spoke can interact only with its hub because the rest of the network (that is, other hubs and spokes) appears hidden behind the hub.

The hub and spoke topology can be adopted for these reasons:
Spoke sites of a VPN customer receives all their traffic from a central (or Hub) site hosting services such as server farms.

Spoke sites of a VPN customer requires all the connectivity between its spoke sites through a central site. This means that the hub site becomes a transit point for interspoke connectivity.

Spoke sites of a VPN customer do not need any connectivity between spoke sites. Hubs can send and receive traffic from all sites but spoke sites can send or receive traffic only to or from Hub sites.

Note
Both Cisco CRS and Cisco XR 12000 Series routers support MVPN v4 Hub-and-spoke implementation. But MVPNv6 Hub-and-spoke is not supported on Cisco CRS Router.

Realizing the Hub and Spoke Topology

Hub and Spoke implementation leverages the infrastructure built for MVPN Extranet. The regular MVPN follows the model in which packets can flow from any site to the other sites. But Hub and Spoke MVPN will restrict traffic flows based on their subscription.

A site can be considered to be a geographic location with a group of CE routers and other devices, such as server farms, connected to PE routers by PE-CE links for VPN access. Either every site can be placed in a separate VRF, or multiple sites can be combined in one VRF on the PE router.

By provisioning every site in a separate VRF, you can simplify the unicast and multicast Hub and Spoke implementation. Such a configuration brings natural protection from traffic leakage - from one spoke site to another. Cisco IOS XR Software implementation of hub and spoke follows the one-site-to-one VRF model. Any site can be designated as either a hub or spoke site, based on how the import or export of routes is setup. Multiple hub and spoke sites can be collated on a given PE router.

Unicast Hub and Spoke connectivity is achieved by the spoke sites importing routes from only Hub sites, and Hub sites importing routes from all sites. As the spoke sites do not exchange routes, spoke to spoke site traffic cannot flow. If interspoke connectivity is required, hubs can choose to re-inject routes learned from one spoke site into other spoke site.

MVPN Hub and Spoke is achieved by separating core tunnels, for traffic sourced from hub sites, and spoke sites. MDT hub is the tunnel carrying traffic sourced from all Hub sites, and MDT spoke carries traffic sourced from all spoke sites. Such tunnel end-points are configured on all PEs participating in hub and spoke topology. If spoke sites do not host any multicast sources or RPs, provisioning of MDT Spoke can be completely avoided at all such routers.

Once these tunnels are provisioned, multicast traffic path will be policy routed in this manner:
1. Hub sites will send traffic to only MDT Hub.
2. Spoke sites will send traffic to only MDT Spoke.
3. Hub sites will receive traffic from both tunnels.
4. Spoke sites will receive traffic from only MDT Hub.

These rules ensure that hubs and spokes can send and receive traffic to or from each other, but direct spoke to spoke communication does not exist. If required, interspoke multicast can flow by turning around the traffic at Hub sites.

These enhancements are made to the Multicast Hub and Spoke topology in Cisco IOS XR Software Release 4.0:

- Auto-RP and BSR are supported across VRFs that are connected through extranet. It is no longer restricted to using static RP only.
• MP-BGP can publish matching import route-targets while passing prefix next-hop information to RIB.
• Route policies can use extended community route targets instead of IP address ranges.
• Support for extranet v4 data mdt was included so that data mdt in hub and spoke can be implemented.

Multicast Source Discovery Protocol

Multicast Source Discovery Protocol (MSDP) is a mechanism to connect multiple PIM sparse-mode domains. MSDP allows multicast sources for a group to be known to all rendezvous points (RPs) in different domains. Each PIM-SM domain uses its own RPs and need not depend on RPs in other domains.

An RP in a PIM-SM domain has MSDP peering relationships with MSDP-enabled routers in other domains. Each peering relationship occurs over a TCP connection, which is maintained by the underlying routing system.

MSDP speakers exchange messages called Source Active (SA) messages. When an RP learns about a local active source, typically through a PIM register message, the MSDP process encapsulates the register in an SA message and forwards the information to its peers. The message contains the source and group information for the multicast flow, as well as any encapsulated data. If a neighboring RP has local joiners for the multicast group, the RP installs the S, G route, forwards the encapsulated data contained in the SA message, and sends PIM joins back towards the source. This process describes how a multicast path can be built between domains.

Note

Although you should configure BGP or Multiprotocol BGP for optimal MSDP interdomain operation, this is not considered necessary in the Cisco IOS XR Software implementation. For information about how BGP or Multiprotocol BGP may be used with MSDP, see the MSDP RPF rules listed in the Multicast Source Discovery Protocol (MSDP), Internet Engineering Task Force (IETF) Internet draft.

Multicast Nonstop Forwarding

The Cisco IOS XR nonstop forwarding (NSF) feature for multicast enhances high availability (HA) of multicast packet forwarding. NSF prevents hardware or software failures on the control plane from disrupting the forwarding of existing packet flows through the router.

The contents of the Multicast Forwarding Information Base (MFIB) are frozen during a control plane failure. Subsequently, PIM attempts to recover normal protocol processing and state before the neighboring routers time out the PIM hello neighbor adjacency for the problematic router. This behavior prevents the NSF-capable router from being transferred to neighbors that will otherwise detect the failure through the timed-out adjacency. Routes in MFIB are marked as stale after entering NSF, and traffic continues to be forwarded (based on those routes) until NSF completion. On completion, MRIB notifies MFIB and MFIB performs a mark-and-sweep to synchronize MFIB with the current MRIB route information.

Note

Nonstop forwarding is not supported for PIM bidirectional routes. If a PIM or MRIB failure (including RP failover) happens with multicast-routing NSF enabled, PIM bidirectional routes in the MFIBs are purged immediately and forwarding on these routes stops. Routes are reinstalled and forwarding recommences after NSF recovery has ended. This affects only bidirectional routes. PIM-SM and
PIM-SSM routes are forwarded with NSF during the failure. This exception is designed to prevent possible multicast routing loops from forming when the control plane is not able to participate in the BiDir Designated Forwarder election.

### Multicast Configuration Submodes

Cisco IOS XR Software moves control plane CLI configurations to protocol-specific submodes to provide mechanisms for enabling, disabling, and configuring multicast features on a large number of interfaces.

Cisco IOS XR Software allows you to issue most commands available under submodes as one single command string from global configuration mode.

For example, the `ssm` command could be executed from the multicast-routing configuration submode like this:

```
RP/0/RP0/CPU0:router(config)# multicast-routing
RP/0/RP0/CPU0:router(config-mcast-ipv4)# ssm range
```

Alternatively, you could issue the same command from global configuration mode like this:

```
RP/0/RP0/CPU0:router(config)# multicast-routing ssm range
```

The following multicast protocol-specific submodes are available through these configuration submodes:

- Multicast-Routing Configuration Submode, page MCC-22
- PIM Configuration Submode, page MCC-22
- IGMP Configuration Submode, page MCC-22
- MLD Configuration Submode, page MCC-23
- MSDP Configuration Submode, page MCC-23

### Multicast-Routing Configuration Submode

When you issue the `multicast-routing ipv4` or `multicast-routing ipv6` command, all default multicast components (PIM, IGMP, MLD, MFWD, and MRIB) are automatically started, and the CLI prompt changes to “config-mcast-ipv4” or “config-mcast-ipv6”, indicating that you have entered multicast-routing configuration submode.

### PIM Configuration Submode

When you issue the `router pim` command, the CLI prompt changes to “config-pim-ipv4,” indicating that you have entered the default pim address-family configuration submode. To enter pim address-family configuration submode for IPv6, type the `address-family ipv6` keyword together with the `router pim` command before pressing Enter.

### IGMP Configuration Submode

When you issue the `router igmp` command, the CLI prompt changes to “config-igmp,” indicating that you have entered IGMP configuration submode.
MLD Configuration Submode

When you issue the `router mld` command, the CLI prompt changes to “config-mld,” indicating that you have entered MLD configuration submode.

MSDP Configuration Submode

When you issue the `router msdp` command, the CLI prompt changes to “config-msdp,” indicating that you have entered router MSDP configuration submode.

Understanding Interface Configuration Inheritance

Cisco IOS XR Software allows you to configure commands for a large number of interfaces by applying command configuration within a multicast routing submode that could be inherited by all interfaces. To override the inheritance mechanism, you can enter interface configuration submode and explicitly enter a different command parameter.

For example, in the following configuration you could quickly specify (under router PIM configuration mode) that all existing and new PIM interfaces on your router will use the hello interval parameter of 420 seconds. However, Packet-over-SONET/SDH (POS) interface 0/1/0/1 overrides the global interface configuration and uses the hello interval time of 210 seconds.

```
RP/0/RP0/CPU0:router(config)# router pim
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# hello-interval 420
RP/0/RP0/CPU0:router(config-pim-default-ipv4)# interface pos 0/1/0/1
RP/0/RP0/CPU0:router(config-pim-ipv4-if)# hello-interval 210
```

The following is a listing of commands (specified under the appropriate router submode) that use the inheritance mechanism:

```
router pim
dr-priority
hello-interval
join-prune-interval

multicast-routing
version
query-interval
query-max-response-time
explicit-tracking
router mld
interface all disable
version
query-interval
query-max-response-time
explicit-tracking

router msdp
connect-source
sa-filter
filter-sa-request list
remote-as
ttl-threshold
```
Understanding Interface Configuration Inheritance Disablement

As stated elsewhere, Cisco IOS XR Software allows you to configure multiple interfaces by applying configurations within a multicast routing submode that can be inherited by all interfaces.

To override the inheritance feature on specific interfaces or on all interfaces, you can enter the address-family IPv4 or IPv6 submode of multicast routing configuration mode, and enter the `interface-inheritance disable` command together with the `interface type interface-path-id` or `interface all` command. This causes PIM or IGMP protocols to disallow multicast routing and to allow only multicast forwarding on those interfaces specified. However, routing can still be explicitly enabled on specified individual interfaces.

The following configuration disables multicast routing interface inheritance under PIM and IGMP generally, although forwarding enablement continues. The example shows interface enablement under IGMP of GigabitEthernet 0/6/0/3:

```
RP/0/RP0/CPU0:router# multicast-routing
RP/0/RP0/CPU0:router(config-mcast-default-ipv4)# interface all enable
RP/0/RP0/CPU0:router(config-mcast-default-ipv4)# interface-inheritance disable
```

For related information, see “Understanding Enabling and Disabling Interfaces”

Understanding Enabling and Disabling Interfaces

When the Cisco IOS XR multicast routing feature is configured on your router, by default, no interfaces are enabled.

To enable multicast routing and protocols on a single interface or multiple interfaces, you must explicitly enable interfaces using the `interface` command in multicast routing configuration mode.

To set up multicast routing on all interfaces, enter the `interface all` command in multicast routing configuration mode. For any interface to be fully enabled for multicast routing, it must be enabled specifically (or be default) in multicast routing configuration mode, and it must not be disabled in the PIM and IGMP/MLD configuration modes.

For example, in the following configuration, all interfaces are explicitly configured from multicast routing configuration submode:

```
RP/0/RP0/CPU0:router(config)# multicast-routing
RP/0/RP0/CPU0:router(config-mcast)# interface all enable
```

To disable an interface that was globally configured from the multicast routing configuration submode, enter interface configuration submode, as illustrated in the following example:

```
RP/0/RP0/CPU0:router(config-mcast)# interface pos 0/1/0/0 disable
```

RP/0/RP0/CPU0:router(config-mcast-default-ipv4-if)# disable
Multicast Routing Information Base

The Multicast Routing Information Base (MRIB) is a protocol-independent multicast routing table that describes a logical network in which one or more multicast routing protocols are running. The tables contain generic multicast routes installed by individual multicast routing protocols. There is an MRIB for every logical network (VPN) in which the router is configured. MRIBs do not redistribute routes among multicast routing protocols; they select the preferred multicast route from comparable ones, and they notify their clients of changes in selected attributes of any multicast route.

Multicast Forwarding Information Base

Multicast Forwarding Information Base (MFIB) is a protocol-independent multicast forwarding system that contains unique multicast forwarding entries for each source or group pair known in a given network. There is a separate MFIB for every logical network (VPN) in which the router is configured. Each MFIB entry resolves a given source or group pair to an incoming interface (IIF) for reverse forwarding (RPF) checking and an outgoing interface list (olist) for multicast forwarding.

MSDP MD5 Password Authentication

MSDP MD5 password authentication is an enhancement to support Message Digest 5 (MD5) signature protection on a TCP connection between two Multicast Source Discovery Protocol (MSDP) peers. This feature provides added security by protecting MSDP against the threat of spoofed TCP segments being introduced into the TCP connection stream.

MSDP MD5 password authentication verifies each segment sent on the TCP connection between MSDP peers. The password command is used to enable MD5 authentication for TCP connections between two MSDP peers. When MD5 authentication is enabled between two MSDP peers, each segment sent on the TCP connection between the peers is verified.

Note

MD5 authentication must be configured with the same password on both MSDP peers; otherwise, the connection between them will not be made.

MSDP MD5 password authentication uses an industry-standard MD5 algorithm for improved reliability and security.

How to Implement Multicast Routing

This section contains instructions for both building a basic multicast configuration, as well as optional tasks to help you to optimize, debug, and discover the routers in your multicast network.

- Configuring PIM-SM and PIM-SSM, page MCC-26 (required)
- Configuring a Static RP and Allowing Backward Compatibility, page MCC-29 (required)
- Configuring Auto-RP to Automate Group-to-RP Mappings, page MCC-31 (optional)
- Configuring the Bootstrap Router, page MCC-33 (optional)
- Calculating Rates per Route, page MCC-37 (optional)
- Configuring Multicast Nonstop Forwarding, page MCC-38 (optional)
Configure PIM-SM and PIM-SSM

PIM is an efficient IP routing protocol that is “independent” of a routing table, unlike other multicast protocols such as Multicast Open Shortest Path First (MOSPF) or Distance Vector Multicast Routing Protocol (DVMRP).

Cisco IOS XR Software supports Protocol Independent Multicast in sparse mode (PIM-SM) and Protocol Independent Multicast in Source-Specific Multicast (PIM-SSM), permitting both to operate on your router at the same time.

**PIM-SM Operations**

PIM in sparse mode operation is used in a multicast network when relatively few routers are involved in each multicast and these routers do not forward multicast packets for a group, unless there is an explicit request for the traffic.

For more information about PIM-SM, see the “PIM-Sparse Mode” section on page MCC-7.

**PIM-SSM Operations**

PIM in Source-Specific Multicast operation uses information found on source addresses for a multicast group provided by receivers and performs source filtering on traffic.

- By default, PIM-SSM operates in the 232.0.0.0/8 multicast group range for IPv4 and ff3x::/32 (where x is any valid scope) in IPv6. To configure these values, use the `ssm range` command.

**Note**

The states that are required for the IPv6-Multicast functionality are also required for the functioning of MVPNv6. There are 48 entries created automatically for each VRF. These entries need to be created in PIM for the proper protocol processing for Joins received within these ranges (either Drop them or consider them as SSM). If there are 1000 such states, which leads to 20 MVRFs, this still will not impact the PE performance. Also, note that these states have Drop flag that does not get affected by MIDB, MGID, and other hardware resources.

- If SSM is deployed in a network already configured for PIM-SM, only the last-hop routers must be upgraded with Cisco IOS XR Software that supports the SSM feature.
- No MSDP SA messages within the SSM range are accepted, generated, or forwarded.

For more information about PIM-SSM, see the “PIM-Source Specific Multicast” section on page MCC-7.
Restrictions for PIM-SM and SSM

Interoperability with SSM
PIM-SM operations within the SSM range of addresses change to PIM-SSM. In this mode, only PIM (S,G) join and prune messages are generated by the router, and no (S,G) RP shared tree or (*,G) shared tree messages are generated.

IGMP Version
To report multicast memberships to neighboring multicast routers, hosts use IGMP, and all routers on the subnet must be configured with the same version of IGMP.

A router running Cisco IOS XR Software does not automatically detect Version 1 systems. You must use the version command in router IGMP configuration submode to configure the IGMP version.

MLD Version
To report multicast memberships to neighboring multicast routers, routers use MLD, and all routers on the subnet must be configured with the same version of MLD.

SUMMARY STEPS

1. configure
2. multicast-routing [address-family {ipv4 | ipv6}]
3. interface all enable
4. exit
5. router {igmp | mld}
6. version {1 | 2 | 3}
7. end or commit
8. show pim [ipv4 | ipv6] group-map [ip-address-name] [info-source]
9. show pim [vrf vrf-name] [ipv4 | ipv6] topology [source-ip-address [group-ip-address] | entry-flag flag | interface-flag | summary] [route-count]

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configure</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RP0/CPU0:router# configure</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>multicast-routing [address-family {ipv4</td>
<td>ipv6}]</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RP0/CPU0:router(config)# multicast-routing</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The following multicast processes are started: MRIB, MFWD, PIM, IGMP, and MLD.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For IPv4, IGMP version 3 is enabled by default; for IPv6, MLD version 1 is enabled by default.</td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step 3</th>
<th>interface all enable</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RP0/CPU0:router(config-mcast-ipv4)# interface all enable</td>
</tr>
<tr>
<td>Purpose</td>
<td>Enables multicast routing and forwarding on all new and existing interfaces.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>exit</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RP0/CPU0:router(config-mcast-ipv4)# exit</td>
</tr>
<tr>
<td>Purpose</td>
<td>Exits multicast routing configuration mode, and returns the router to the source configuration mode.</td>
</tr>
</tbody>
</table>

| Step 5 | router {igmp | mld} |
|--------|----------------------|
| **Example:** | RP/0/RP0/CPU0:router(config)# router igmp |
| Purpose | (Optional) Enters router IGMP or MLD configuration mode. |

| Step 6 | version {1 | 2 | 3} |
|--------|----------------------|
| **Example:** | RP/0/RP0/CPU0:router(config-igmp)# version 3 |
| Purpose | (Optional) Selects the IGMP or MLD version that the router interface uses. |
|  &bull; | The default for IGMP is version 3; the default for MLD is version 1. |
|  &bull; | Host receivers must support IGMPv3 for PIM-SSM operation. |
|  &bull; | If this command is configured in router IGMP or router MLD configuration mode, parameters are inherited by all new and existing interfaces. You can override these parameters on individual interfaces from interface configuration mode. |

<table>
<thead>
<tr>
<th>Step 7</th>
<th>end or commit</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RP0/CPU0:router(config-igmp)# end</td>
</tr>
<tr>
<td></td>
<td>RP/0/RP0/CPU0:router(config-igmp)# commit</td>
</tr>
<tr>
<td>Purpose</td>
<td>Saves configuration changes.</td>
</tr>
<tr>
<td>•</td>
<td>When you issue the <strong>end</strong> command, the system prompts you to commit changes:</td>
</tr>
<tr>
<td>•</td>
<td>Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:</td>
</tr>
<tr>
<td>•</td>
<td>- Entering <strong>yes</strong> saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.</td>
</tr>
<tr>
<td>•</td>
<td>- Entering <strong>no</strong> exits the configuration session and returns the router to EXEC mode without committing the configuration changes.</td>
</tr>
<tr>
<td>•</td>
<td>- Entering <strong>cancel</strong> leaves the router in the current configuration session without exiting or committing the configuration changes.</td>
</tr>
<tr>
<td>•</td>
<td>Use the <strong>commit</strong> command to save the configuration changes to the running configuration file and remain within the configuration session.</td>
</tr>
</tbody>
</table>
Implementing Multicast Routing on Cisco IOS XR Software

How to Implement Multicast Routing

Configuring a Static RP and Allowing Backward Compatibility

When PIM is configured in sparse mode, you must choose one or more routers to operate as a rendezvous point (RP) for a multicast group. An RP is a single common root placed at a chosen point of a shared distribution tree. An RP can either be configured statically in each router, or learned through Auto-RP or BSR.

This task configures a static RP. For more information about RPs, see the “Rendezvous Points” section on page MCC-11. For configuration information for Auto-RP, see the “Configuring Auto-RP to Automate Group-to-RP Mappings” section on page MCC-31.

SUMMARY STEPS

1. configure
2. router pim [address-family {ipv4 | ipv6}]
3. rp-address ip-address [group-access-list] [bidir] [override]
4. old-register-checksum
5. exit
6. {ipv4 | ipv6} access-list name
7. [sequence-number] permit any source [source-wildcard]
8. end or commit
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RP0/CPU0:router# configure</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> router pim [address-family {ipv4</td>
<td>ipv6}]</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RP0/CPU0:router(config)# router pim</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> rp-address ip-address [group-access-list] [bidir] [override]</td>
<td>Assigns an RP to multicast groups.</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RP0/CPU0:router(config-pim-default-ipv4)# rp-address 172.16.6.22 rp-access</td>
<td>• If you specify a group-access-list-number value, you must configure that access list using the ipv4 access-list command.</td>
</tr>
<tr>
<td><strong>Step 4</strong> old-register-checksum</td>
<td>(Optional) Allows backward compatibility on the RP that uses old register checksum methodology.</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RP0/CPU0:router(config-pim-ipv4)# old-register-checksum</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> exit</td>
<td>Exits PIM configuration mode, and returns the router to the source configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RP0/CPU0:router(config-pim-ipv4)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> {(ipv4</td>
<td>ipv6)} access-list name</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RP0/CPU0:router(config)# ipv4 access-list rp-access</td>
<td>• The access list called “rp-access” permits multicast group 239.1.1.0 0.0.255.255.</td>
</tr>
</tbody>
</table>
Configuring Auto-RP to Automate Group-to-RP Mappings

This task configures the Auto-RP mechanism to automate the distribution of group-to-RP mappings in your network. In a network running Auto-RP, at least one router must operate as an RP candidate and another router must operate as an RP mapping agent.

For more information about Auto-RP, see the “Auto-RP” section on page MCC-12.

SUMMARY STEPS

1. configure
2. router pim [address-family ipv4 | ipv6]
3. auto-rp candidate-rp type instance scope ttl-value [group-list access-list-name] [interval seconds]
4. auto-rp mapping-agent type number scope ttl-value [interval seconds]
5. exit

---

**Command or Action**

**Purpose**

**Step 7**

(sequence-number) permit any source [source-wildcard]

(Optional) Permits multicast group 239.1.1.0 0.0.255.255 for the “rp-access” list.

**Example:**

RP/0/RP0/CPU0:router(config-ipv4-acl)# permit any 239.1.1.0 0.0.255.255

**Tip**

The commands in Step 6 and Step 7 can be combined in one command string and entered from global configuration mode like this: ipv4 access-list rp-access permit 239.1.1.0 0.0.255.255.

**Note**

There must be one “any” in order to successfully commit the [group-access-list]. Deny statements are ignored.

**Step 8**

end or commit

Saves configuration changes.

- When you issue the end command, the system prompts you to commit changes:

  Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:

  - Entering yes saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
  - Entering no exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
  - Entering cancel leaves the router in the current configuration session without exiting or committing the configuration changes.

- Use the commit command to save the configuration changes to the running configuration file and remain within the configuration session.
6. `ipv4 access-list name`
7. `[sequence-number] permit source [source-wildcard]`
8. `end` or `commit`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RP0/CPU0::router# configure</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> router pim [address-family ipv4</td>
<td>ipv6]</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RP0/CPU0:router(config)# router pim</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> auto-rp candidate-rp type instance scope ttl-value [group-list access-list-name] [interval seconds]</td>
<td>Configures an RP candidate that sends messages to the CISCO-RP-ANNOUNCE multicast group (224.0.1.39).</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RP0/CPU0:router(config-pim-ipv4)# auto-rp candidate-rp GigabitEthernet0/1/0/1 scope 31 group-list 2</td>
<td>- This example sends RP announcements out all PIM-enabled interfaces for a maximum of 31 hops. The IP address by which the router wants to be identified as an RP is the IP address associated with GigabitEthernet interface 0/1/0/1.</td>
</tr>
<tr>
<td><strong>Step 4</strong> auto-rp mapping-agent type number scope ttl-value [interval seconds]</td>
<td>Configures the router to be an RP mapping agent on a specified interface.</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RP0/CPU0::router(config-pim-ipv4)# auto-rp mapping-agent GigabitEthernet0/1/0/1 scope 20</td>
<td>- After the router is configured as an RP mapping agent and determines the RP-to-group mappings through the CISCO-RP-ANNOUNCE (224.0.1.39) group, the router sends the mappings in an Auto-RP discovery message to the well-known group CISCO-RP-DISCOVERY (224.0.1.40).</td>
</tr>
<tr>
<td><strong>Step 5</strong> exit</td>
<td>Exits PIM configuration mode and returns the router to the source configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RP0/CPU0::router(config-pim-ipv4)# exit</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring the Bootstrap Router

This task configures one or more candidate bootstrap routers (BSRs) and a BSR mapping agent. This task also connects and locates the candidate BSRs in the backbone portion of the network.

For more information about BSR see the “PIM Bootstrap Router” section on page MCC-12.

### SUMMARY STEPS

1. configure
2. router pim [address-family {ipv4 | ipv6}]
3. bsr candidate-bsr ip-address [hash-mask-len length] [priority value]
4. bsr candidate-rp ip-address [group-list access-list] [interval seconds] [priority value]
5. interface type interface-path-id
6. bsr border

### CONFIGURATION STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 6</strong></td>
<td>extents travelled from the source to the RP, and restricts unrelated multicast traffic.</td>
</tr>
<tr>
<td><code>ipv4 access-list name</code></td>
<td>(Optional) Defines the RP access list.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RP0/CPU0:router(config)# ipv4 access-list 2</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>The commands in Step 6 and Step 7 can be combined in one command string and entered from global configuration mode like this: ipv4 access-list rp-access permit 239.1.1.1 0.0.0.0</td>
</tr>
<tr>
<td><code>[sequence-number] permit source [source-wildcard]</code></td>
<td>(Optional) Permits multicast group 239.1.1.1 for the RP access list.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RP0/CPU0:router(config-ipv4-acl)# permit 239.1.1.1 0.0.0.0</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>Saves configuration changes.</td>
</tr>
<tr>
<td><code>end</code></td>
<td>When you issue the end command, the system prompts you to commit changes:</td>
</tr>
<tr>
<td><code>commit</code></td>
<td>Uncommitted changes found, commit them before exiting (yes/no/cancel)? [cancel]:</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RP0/CPU0:router(config-ipv4-acl)# end or RP/0/RP0/CPU0:router(config-ipv4-acl)# commit</td>
</tr>
<tr>
<td><strong>Tip</strong></td>
<td>– Entering yes saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>– Entering no exits the configuration session and returns the router to EXEC mode without committing the configuration changes.</td>
</tr>
<tr>
<td></td>
<td>– Entering cancel leaves the router in the current configuration session without exiting or committing the configuration changes.</td>
</tr>
<tr>
<td></td>
<td>• Use the commit command to save the configuration changes to the running configuration file and remain within the configuration session.</td>
</tr>
</tbody>
</table>
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>RP/0/RP0/CPU0:router# configure</td>
</tr>
<tr>
<td>2</td>
<td>router pim [address-family {ipv4</td>
<td>ipv6}]</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>RP/0/RP0/CPU0:router(config)# router pim</td>
</tr>
<tr>
<td>3</td>
<td>bsr candidate-bsr ip-address [hash-mask-len] length [priority value]</td>
<td>Configures the router to announce its candidacy as a BSR.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>RP/0/RP0/CPU0:router(config-pim-default-ipv4)# bsr candidate-bsr 10.0.0.1 hash-mask-len 30</td>
</tr>
<tr>
<td>4</td>
<td>bsr candidate-rp ip-address [group-list access-list] [interval seconds] [priority value]</td>
<td>Configures the router to advertise itself as a PIM Version 2 candidate RP to the BSR.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>RP/0/RP0/CPU0:router(config-pim-default-ipv4)# bsr candidate-rp 172.16.0.0 group-list 4</td>
</tr>
<tr>
<td>5</td>
<td>interface type interface-path-id</td>
<td>(Optional) Enters interface configuration mode for the PIM protocol.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>RP/0/RP0/CPU0:router(config-pim-default-ipv4)# interface GigE 0/1/0/0</td>
</tr>
<tr>
<td>Step 6</td>
<td><code>bsr-border</code></td>
<td>(Optional) Stops the forwarding of bootstrap router (BSR) messages on a Protocol Independent Multicast (PIM) router interface.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RP0/CPU0:router(config-pim-ipv4-if)# bsr-border</td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td><code>exit</code></td>
<td>(Optional) Exits PIM interface configuration mode, and returns the router to PIM configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RP0/CPU0:router(config-pim-ipv4-if)# exit</td>
<td></td>
</tr>
<tr>
<td>Step 8</td>
<td><code>exit</code></td>
<td>Exits PIM configuration mode, and returns the router to global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RP0/CPU0:router(config-pim-default-ipv4)# exit</td>
<td></td>
</tr>
<tr>
<td>Step 9</td>
<td>`{ipv4</td>
<td>ipv6} access-list name`</td>
</tr>
</tbody>
</table>
| **Example:** | RP/0/RP0/CPU0:router(config)# ipv4 access-list 4 | - Access list number 4 specifies the group prefix associated with the candidate RP address 172.16.0.0. (See Step 4).  
- This RP is responsible for the groups with the prefix 239. |
| Step 10 | `[sequence-number] permit source [source-wildcard] any`  
or  
`[sequence-number] permit any source-prefix dest-prefix` | (Optional) Permits multicast group 239.1.1.1 for the candidate group list. |
| **Example:** | RP/0/RP0/CPU0:router(config-ipv4-acl)# permit any 239.1.1.1 0.255.255.255 | Tip: The commands in Step 6 and Step 7 can be combined in one command string and entered from global configuration mode like this: ipv4 access-list rp-access permit 239.1.1.1 0.255.255.255 |
| Note | There must be one “any” in order to successfully commit the [group-access-list]. Deny statements are ignored. |
## Step 11
### end
or
### commit

**Example:**
```
RP/0/RP0/CPU0:router(config-ipv4-acl)# end
RP/0/RP0/CPU0:router(config-ipv4-acl)# commit
```

- **Purpose:** Saves configuration changes.
  - When you issue the **end** command, the system prompts you to commit changes:
    - Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:
      - Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
      - Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
      - Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.
  - Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

## Step 12
### clear pim [vrf vrf-name] [ipv4 | ipv6] bsr

**Example:**
```
RP/0/RP0/CPU0:router# clear pim bsr
```

- **Purpose:** (Optional) Clears BSR entries from the PIM RP group mapping cache.

## Step 13
### show pim [vrf vrf-name] [ipv4 | ipv6] bsr candidate-rp

**Example:**
```
RP/0/RP0/CPU0:router# show pim bsr candidate-rp
```

- **Purpose:** (Optional) Displays PIM candidate RP information for the BSR.

## Step 14
### show pim [vrf vrf-name] [ipv4 | ipv6] bsr election

**Example:**
```
RP/0/RP0/CPU0:router# show pim bsr election
```

- **Purpose:** (Optional) Displays PIM candidate election information for the BSR.

## Step 15
### show pim [vrf vrf-name] [ipv4 | ipv6] bsr rp-cache

**Example:**
```
RP/0/RP0/CPU0:router# show pim bsr rp-cache
```

- **Purpose:** (Optional) Displays PIM RP cache information for the BSR.

## Step 16
### show pim [vrf vrf-name] [ipv4 | ipv6] group-map [ip-address-name] [info-source]

**Example:**
```
RP/0/RP0/CPU0:router# show pim ipv4 group-map
```

- **Purpose:** (Optional) Displays group-to-PIM mode mapping.

### Note
A group range indicates how PIM maps a group to its RP. Both IPv4 and IPv6 PIM create several internal group ranges. For IPv6 PIM, the multicast scopes 0,1, and 2 are not routable, so group ranges are created to cover those. Additionally, group ranges are created for the embedded RP group ranges and for the SSM groups.
## Calculating Rates per Route

This procedure enables multicast hardware forward-rate counters on a per-VRF-family basis.

### SUMMARY STEPS

1. `configure`
2. `multicast-routing [vrf vrf-name] [address-family {ipv4 | ipv6}]`
3. `rate-per-route`
4. `interface {type interface-path-id | all} enable`
5. `accounting per-prefix or accounting per-prefix forward-only`
6. `end` or `commit`
7. `show mfib [vrf vrf-name] [ipv4 | ipv6] route [rate | statistics] [* | source-address] [group-address [/prefix-length] | detail | old-output] | summary] [location node-id]

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure</strong>&lt;br&gt;Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>RP/0/RP0/CPU0:router# configure</code></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>**multicast-routing [vrf vrf-name] [address-family {ipv4</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>RP/0/RP0/CPU0:router(config)# multicast-routing address-family ipv4</code></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>rate-per-route</strong>&lt;br&gt;Enables a per (S,G) rate calculation for a particular route.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>RP/0/RP0/CPU0:router(config-mcast-default-ipv4)# rate-per-route</code></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>**interface {type interface-path-id</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>RP/0/RP0/CPU0:router(config-mcast-default-ipv4)# interface all enable</code>&lt;br&gt;or&lt;br&gt;<code>RP/0/RP0/CPU0:router(config-mcast-default-ipv4)# interface FastEthernet0/3/3/1 enable</code></td>
</tr>
</tbody>
</table>
## How to Implement Multicast Routing

### Command or Action

**Step 5**

- accounting per-prefix
  - or
  - accounting per-prefix forward-only

**Example:**

```
RP/0/RP0/CPU0:router(config-mcast-default-ipv4)#
accounting per-prefix
```

**Step 6**

- end
  - or
  - commit

**Example:**

```
RP/0/RP0/CPU0:router(config-mcast-default-ipv4)# end
```

### Purpose

- Enables per-prefix counters present in hardware accounting per-prefix—Enables three counters on ingress (forward, punt and drop, and two on egress (forward and punt) on every existing and new (S, G) route. The (*, G) routes are assigned a single counter.
- accounting per-prefix forward-only—Enables one counter on ingress and one on egress in hardware to conserve hardware statistics resources. (Recommended for configuration of multicast VPN routing or for any line card that has a route-intensive configuration.)

### Command or Action

**Step 7**

- show mfib [vrf vrf-name] [ipv4 | ipv6] route
  - [rate | statistics] [* | source-address]
  - [group-address [/prefix-length] | detail | old-output] | summary] [location node-id]

**Example:**

```
RP/0/RP0/CPU0:router# show mfib vrf 12 route
statistics location 0/1/cpU0
```

### Purpose

- Displays route entries in the Multicast Forwarding Information Base (MFIB) table.
  - When the **rate** keyword is used with the **source-** and **group-address**, the command displays the cumulative rates per route for all line cards in the Multicast Forwarding Information Base (MFIB) table.
  - When the **statistics** keyword is used, the command displays the rate per route for one line card in the Multicast Forwarding Information Base (MFIB) table.

## Configuring Multicast Nonstop Forwarding

This task configures the nonstop forwarding (NSF) feature for multicast packet forwarding for the purpose of alleviating network failures, or software upgrades and downgrades.
Although we strongly recommend that you use the NSF lifetime default values, the optional Step 4 through Step 9 allow you to modify the NSF timeout values for Protocol Independent Multicast (PIM) and Internet Group Management Protocol (IGMP) or Multicast Listener Discovery (MLD). Use these commands when PIM and IGMP or MLD are configured with nondefault interval or query intervals for join and prune operations.

Generally, configure the IGMP NSF and PIM NSF lifetime values to equal or exceed the query or join query interval. For example, if you set the IGMP query interval to 120 seconds, set the IGMP NSF lifetime to 120 seconds (or greater).

If the Cisco IOS XR Software control plane does not converge and reconnect after NSF is enabled on your router, multicast packet forwarding continues for up to 15 minutes, then packet forwarding stops.

**Prerequisites for Multicast Nonstop Forwarding**

For NSF to operate in your multicast network, you must also enable NSF for the unicast protocols (such as IS-IS, OSPF, and BGP) that PIM relies on for Reverse Path Forwarding (RPF) information. See the appropriate configuration modules to learn how to configure NSF for unicast protocols.

**SUMMARY STEPS**

1. configure
2. multicast-routing [address-family {ipv4 | ipv6}]
3. nsf [lifetime seconds]
4. exit
5. router pim [address-family {ipv4| ipv6}]
6. nsf lifetime seconds
7. exit
8. router {igmp | mld}
9. nsf lifetime seconds
10. end or commit
11. show {igmp | mld} [old-output] nsf
12. show mfib [ipv4| ipv6] nsf [location node-id]
13. show mrib [ipv4| ipv6] [old-output] nsf
14. show pim [ipv4| ipv6] nsf
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RP0/CPU0:router# configure</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> multicast-routing [address-family {ipv4</td>
<td>ipv6}]</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RP0/CPU0:router(config)# multicast-routing</td>
<td>- The following multicast processes are started: MRIB, MFWD, PIM, IGMP, and MLD.</td>
</tr>
<tr>
<td></td>
<td>- For IPv4, IGMP version 3 is enabled by default; for IPv6, MLD version 1 is enabled by default.</td>
</tr>
<tr>
<td><strong>Step 3</strong> nsf [lifetime seconds]</td>
<td>Turns on NSF capability for the multicast routing system.</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RP0/CPU0:router(config-mcast)# nsf</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> exit</td>
<td>(Optional) Exits multicast routing configuration mode, and returns the router to the source configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RP0/CPU0:router(config-mcast)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> router pim [address-family {ipv4</td>
<td>ipv6}]</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RP0/CPU0:router(config)# router pim address-family ipv4</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> nsf lifetime seconds</td>
<td>(Optional) Configures the NSF timeout value for multicast forwarding route entries under the PIM process.</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RP0/CPU0:router(config-pim-default-ipv4)# nsf lifetime 30</td>
<td><strong>Note</strong> If you configure the PIM hello interval to a nondefault value, configure the PIM NSF lifetime to a value less than the hello hold time. Typically the value of the hold-time field is 3.5 times the interval time value, or 120 seconds if the PIM hello interval time is 30 seconds.</td>
</tr>
<tr>
<td><strong>Step 7</strong> exit</td>
<td>(Optional) Exits PIM configuration mode and returns the router to the source configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RP0/CPU0:router(config-pim-default-ipv4)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> router {igmp</td>
<td>mld}</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RP0/CPU0:router(config)# router igmp</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action | Purpose |
|------------------------|----------|
| **Step 9**
  nsf lifetime seconds | (Optional) Configures the NSF timeout value for multicast forwarding route entries under the IGMP or MLD process. |
| Example:
  RP/0/RP0/CPU0:router(config-igmp)# nsf lifetime 30 | |
| **Step 10**
  end
  or
  commit | Saves configuration changes. |
| Example:
  RP/0/RP0/CPU0:router(config-igmp)# end
  or
  RP/0/RP0/CPU0:router(config-igmp)# commit | |
| **Step 11**
  show {igmp | mld} [old-output] nsf | (Optional) Displays the state of NSF operation in IGMP or MLD. |
| Example:
  RP/0/RP0/CPU0:router# show igmp nsf | |
| **Step 12**
  show mfib [ipv4 | ipv6] nsf [location node-id] | (Optional) Displays the state of NSF operation for the MFIB line cards. |
| Example:
  RP/0/RP0/CPU0:router# show mfib nsf | |
| **Step 13**
  show mrib [ipv4 | ipv6] [old-output] nsf | (Optional) Displays the state of NSF operation in the MRIB. |
| Example:
  RP/0/RP0/CPU0:router# show mrib nsf | |
| **Step 14**
  show pim [ipv4 | ipv6] nsf | (Optional) Displays the state of NSF operation for PIM. |
| Example:
  RP/0/RP0/CPU0:router# show pim nsf | |

### Configuring Multicast VPN

- Enabling a VPN for Multicast Routing, page MCC-43 (required)
- “Configuring BGP to Advertise VRF Routes for Multicast VPN from PE to PE” (required)
See the module “Implementing BGP on Cisco IOS XR Software” in Cisco IOS XR Routing Configuration Guide.

- Configuring an MDT Address Family Session in BGP as a PE-to-PE Protocol (optional for PIM-SM MDT groups; required for PIM-SSM MDT groups)
  See the “Configuring an MDT Address Family Session in BGP” section in Cisco IOS XR Routing Configuration Guide.

- Configuring a provider-edge-to-customer-edge protocol (optional)
  See the “Configuring BGP as a PE-CE Protocol,” “Configuring OSPF as a PE-to-CE Protocol,” and “Configuring EIGRP as a PE-to-CE Protocol” sections in Cisco IOS XR Routing Configuration Guide.

- Specifying the PIM VRF Instance, page MCC-45 (optional)
- Specifying the IGMP VRF Instance, page MCC-46 (optional)
- Configuring the MDT Source per VRF, page MCC-47 (optional)

For an examples of end-to-end MVPN configuration, see Configuring IPv4 Multicast VPN: Example, page MCC-74.

### Prerequisites for Multicast VPN

- PIM and multicast forwarding must be configured on all interfaces used by multicast traffic. In an MVPN, you must enable PIM and multicast forwarding for the following interfaces:
  - Physical interface on a provider edge (PE) router that is connected to the backbone.
  - Interface used for BGP peering source address.
  - Any interfaces configured as PIM rendezvous points.

  **Note** PIM and multicast forwarding are enabled in multicast routing configuration mode. No additional configuration is required in router pim mode to enable the PIM protocol.

- Interfaces in the VPN intended for use in forwarding multicast traffic must be enabled for PIM and multicast forwarding.

- BGP should already be configured and operational on all routers that are sending or receiving multicast traffic.

- To enable MVPN, you must include a VPN IPv4 address-family (AFI) in your BGP configuration. See Restrictions for Multicast VPN for Multicast Routing, page MCC-43. (See also the “Enabling BGP Routing” section in Cisco IOS XR Routing Configuration Guide.)

- All PE routers in the multicast domain must be running a Cisco IOS XR software image that supports MVPN.

- Multicast forwarding must be configured for the global IPv4 address family.

- Each multicast SM VRF domain must have an associated PIM rendezvous point (RP) definition. Using Auto-RP and the bootstrap router (BSR), you may configure RP services in the MVPN on the customer-edge (CE) device because the MVPN learns about the RP dynamically. The VRF interface can be used as a listener on the PE device.

  To enable static RP services, you must configure every device in the domain for this purpose.
Restrictions for Multicast VPN for Multicast Routing

- Configuration of the MDT source on a per-VRF basis is only supported on IPv4.

Enabling a VPN for Multicast Routing

This task enables multicast VPN routing for IPv4.

The MDT group address is used by provider edge (PE) routers to form a virtual PIM “neighborship” for the MDT. This enables the PEs to communicate with other PEs in the VRF as if they shared a LAN.

When sending customer VRF traffic, PEs encapsulate the traffic in their own (S,G) state, where the G is the MDT group address, and the S is the MDT source for the PE. By joining the (S,G) MDT of its PE neighbors, a PE router is able to receive the encapsulated multicast traffic for that VRF.

Although the VRF itself may have many multicast sources sending to many groups, the provider network needs only to install state for one group per VRF, in other words, the MDT group.

SUMMARY STEPS

1. configure
2. multicast-routing
3. address-family ipv4
4. nsf
5. mdt source type interface-path-id
6. interface all enable
7. vrf vrf-name [address-family {ipv4}]
8. mdt default mdt-group-address
9. mdt data mdt-group-address/prefix-length threshold threshold acl-name
10. interface all enable
11. end or commit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
configure

Example:
RP/0/CP0/CPU0:router# configure

Enters global configuration mode. |
| **Step 2**
multicast-routing

Example:
RP/0/CP0/CPU0:router(config)# multicast-routing |

Enters multicast routing configuration mode. |
### How to Implement Multicast Routing

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>address-family ipv4</td>
<td><strong>Note</strong> Enters ipv4 address-family submode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> RP/0/CP0/CPU0:router(config-mcast)# address-family ipv4</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>nsf</td>
<td>Specifies that nonstop forwarding (NSF) maintains the forwarding state in case of a disruption to a multicast process.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> RP/0/CP0/CPU0:router(config-mcast-default-ipv4)# nsf</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>mdt source type interface-path-id</td>
<td>Specifies the MDT source address. <strong>Note</strong> The MDT source interface is recommended to use BGP peering update-source interface, however, can also use another interface in default VRF.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> RP/0/CP0/CPU0:router(config-mcast-default-ipv4)# mdt source GigE 0/1/0/0</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>interface all enable</td>
<td>Enables multicast routing and forwarding on all new and existing interfaces. You can also enable individual interfaces. <strong>Caution</strong> To avoid any possibility of a reverse-path forwarding (RPF) failure, you should proactively enable any interfaces that might possibly carry multicast traffic.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> RP/0/CP0/CPU0:router(config-mcast-default-ipv4)# interface all enable</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>vrf vrf-name</td>
<td>Configures a VPN routing and forwarding (VRF) instance and enters VRF configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> RP/0/CP0/CPU0:router(config-mcast-default-)# vrf vrf_A</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>vrf vrf_A [address-family (ipv4)]</td>
<td>Specifies the virtual routing and forwarding instance for the ipv4 address family.</td>
</tr>
<tr>
<td>9</td>
<td>mdt default mdt-group-address</td>
<td>Specifies the multicast distribution tree (MDT) default group address. <strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> RP/0/CP0/CPU0:router(config-mcast-vrf_A-ipv4)# mdt default 239.23.2.1</td>
<td></td>
</tr>
</tbody>
</table>
Specifying the PIM VRF Instance

If you are configuring Protocol Independent Multicast in sparse mode (PIM-SM) in the MVPN, you may also need to configure a rendezvous point (RP). This task specifies the optional PIM VPN instance.

SUMMARY STEPS

1. configure
2. router pim vrf vrf-name address-family{ipv4 | ipv6}
3. rp-address ip-address [group-access-list-number] [override]
4. end or commit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RP0/CPU0:router# configure</td>
</tr>
<tr>
<td>Step 2 router pim vrf vrf-name address-family {ipv4</td>
<td>ipv6}</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RP0/CPU0:router(config)# router pim vrf vrf_A address-family ipv4</td>
</tr>
<tr>
<td>Step 3 rp-address ip-address [group-access-list-name] [bidir] [override]</td>
<td>Configures the PIM rendezvous point (RP) address:</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RP0/CPU0:router(config-pim-vrf_A-ipv4)# rp-address 10.0.0.0</td>
</tr>
<tr>
<td>Step 4 end or commit</td>
<td>Saves configuration changes.</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RP0/CPU0:router(config-pim-vrf_A-ipv4)# end or RP/0/RP0/CPU0:router(config-pim-vrf_A-ipv4)# commit</td>
</tr>
</tbody>
</table>

Specifying the IGMP VRF Instance

SUMMARY STEPS

1. configure
2. `router igmp`
3. `vrf vrf-name`
4. `end` or `commit`

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure</code> &lt;br&gt; Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RP0/CPU0:router# configure</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>router igmp</code> &lt;br&gt; Enters IGMP configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RP0/CPU0:router(config)# router igmp</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>vrf vrf-name</code> &lt;br&gt; Configures a VRF instance.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RP0/CPU0:router(config-igmp)# vrf vrf_B</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>end</code> or <code>commit</code> &lt;br&gt; Saves configuration changes. &lt;br&gt; • When you issue the <code>end</code> command, the system prompts you to commit changes: &lt;br&gt; Uncommitted changes found, commit them before exiting (yes/no/cancel)? [cancel]: &lt;br&gt; – Entering <strong>yes</strong> saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode. &lt;br&gt; – Entering <strong>no</strong> exits the configuration session and returns the router to EXEC mode without committing the configuration changes. &lt;br&gt; – Entering <strong>cancel</strong> leaves the router in the current configuration session without exiting or committing the configuration changes. &lt;br&gt; • Use the <code>commit</code> command to save the configuration changes to the running configuration file and remain within the configuration session.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RP0/CPU0:router(config-igmp-vrf_B)# end or RP/0/RP0/CPU0:router(config-igmp-vrf_B)# commit</td>
</tr>
</tbody>
</table>

Configuring the MDT Source per VRF

This optional feature lets you change the default routing mechanism in a multicast VPN network topology, which routes all unicast traffic through a BGP peering loopback configured on a default VRF. Instead, you may configure a loopback that allows you to specify the MDT source using a specific VRF, as opposed to the default VRF. This overrides the current behavior and updates BGP as part of a MDT group. BGP then modifies the source and connector attributes in the MDT SAFI and VPN IPv4 updates.
For VRFs on which the MDT source is not configured, the MDT source for the default VRF is applied. Also, when the MDT source on a VRF is unconfigured, the configuration of the MDT source default VRF takes effect.

Note
In the configuration below, the default VRF does not require explicit reference in Step 3.

SUMMARY STEPS

1. configure
2. multicast-routing
3. mdt source interface type interface-path-id

Note
This is the default VRF.

4. vrf vrf-name mdt source loopback interface-path-id

Note
This is the first specified VRF.

5. Repeat the foregoing step as many times as needed to create other VRFs.
6. end or commit
7. show pim vrf all mdt interface

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RP0/CPU0:router# configure</td>
</tr>
<tr>
<td>Step 2 multicast-routing</td>
<td>Enables IP multicast routing and forwarding.</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RP0/CPU0:router(config)#</td>
</tr>
<tr>
<td></td>
<td>multicast-routing</td>
</tr>
<tr>
<td></td>
<td>RP/0/RP0/CPU0:router(config-mcast)#</td>
</tr>
<tr>
<td>Step 3 mdt source loopback interface-path-id</td>
<td>Configures the interface used to set the MDT source address for MVPN, using the default VRF.</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RP0/CPU0:router(config-mcast)#</td>
</tr>
<tr>
<td></td>
<td>mdt source loopback 0</td>
</tr>
<tr>
<td></td>
<td>Note</td>
</tr>
<tr>
<td></td>
<td>The MDT source command under default VRF is required to enable MVPN.</td>
</tr>
</tbody>
</table>
### Step 4

**Command or Action**

```
 vrf vrf-name mdt source loopback
  interface-path-id
```

**Purpose**

Configures a second interface by specifying a particular VRF on a loopback to override the default VRF.

**Example:**

```
RP/0/RP0/CPU0:router(config-mcast)#
vrf 101 mdt source loopback 1
```

### Step 5

**Repeat the foregoing step as many times as needed to create other VRFs.**

**Example:**

```
RP/0/RP0/CPU0:router(config-mcast)#
vrf 102 mdt source loopback 2
```

### Step 6

**end or commit**

**Example:**

```
RP/0/RP0/CPU0:router(config-mcast)#
commit
```

**Purpose**

Saves configuration changes.

- When you issue the **end** command, the system prompts you to commit changes:

  Uncommitted changes found, commit them before exiting (yes/no/cancel)? [cancel]:

  - Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
  - Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
  - Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.

- Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

### Step 7

**Command or Action**

```
show pim vrf all mdt interface
```

**Example:**

```
RP/0/RP0/CPU0:router# show pim vrf all mdt interface
```

**Purpose**

Displays all MDT data streams.

In this example, loopback 1 is the per-VRF MDT source.
Configuring Multitopology Routing

This set of procedures configures multitopology routing, which is used by PIM for reverse-path forwarding (RPF) path selection.

- “Configuring a Global Topology and Associating It with an Interface” (required)
  For information, see Cisco IOS XR Routing Configuration Guide.
- “Enabling an IS-IS Topology” (required)
  For information, see Cisco IOS XR Routing Configuration Guide.
- “Placing an Interface in a Topology in IS-IS” (required)
  For information, see Cisco IOS XR Routing Configuration Guide.
- “Configuring a Routing Policy” (required)
  For information, see Cisco IOS XR Routing Configuration Guide.
- “Configuring an RPF Topology in PIM” section on page MCC-51 (required)
  For an example of multitopology routing, see Configuring Multitopology Routing: Example, page MCC-84.

Restrictions for Configuring Multitopology Routing

- Only the default VRF is currently supported in a multitopology solution.
- Only protocol-independent multicast (PIM) and intermediate system-intermediate system (IS-IS) routing protocols are currently supported.
- Topology selection is restricted solely to (S, G) route sources for both SM and SSM. Static and IS-IS are the only interior gateway protocols (IGPs) that support multitopology deployment.

  For non-(S, G) route sources like a rendezvous point or bootstrap router (BSR), or when a route policy is not configured, the current policy default remains in effect. In other words, either a unicast-default or multicast-default table is selected for all sources based on any of the following configurations:
  - Open Shortest Path First (OSPF)
  - Intermediate System-to-Intermediate System (IS-IS)
  - Multiprotocol Border Gateway Protocol (MBGP)

Note

Although both multicast and unicast keywords are available when using the address-family {ipv4 | ipv6} command in routing policy language (RPL), only topologies under multicast SAFI can be configured globally.

Information About Multitopology Routing

Configuring multitopology networks requires the following tasks:

- “Configuring a Global Topology and Associating It with an Interface” (required)
  For information, see Cisco IOS XR Routing Configuration Guide.
- “Enabling an IS-IS Topology” (required)
  For information, see Cisco IOS XR Routing Configuration Guide.
• “Placing an Interface in a Topology in IS-IS” (required)
  For information, see Cisco IOS XR Routing Configuration Guide.
• “Configuring a Routing Policy” (required)
  For information, see Cisco IOS XR Routing Configuration Guide.
• “Configuring an RPF Topology in PIM” section on page MCC-51 (required)
  For an example of multitopology routing, see Configuring Multitopology Routing: Example, page MCC-84.

Configuring an RPF Topology in PIM

SUMMARY STEPS

1. configure
2. router pim address-family {ipv4 | ipv6}
3. rpf topology route-policy policy-name
4. exit
5. multicast-routing address family {ipv4 | ipv6}
6. interface all enable
7. end or commit
8. show pim [vrf vrf-name] [ipv4 | ipv6] [{unicast | multicast | safi-all} topology {table-name | all}] rpf [ip-address | hash | summary | route-policy]

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: RP/0/RP0/CPU0:router# configure</td>
<td></td>
</tr>
<tr>
<td>Step 2 router pim address-family (ipv4</td>
<td>ipv6)</td>
</tr>
<tr>
<td>Example: RP/0/RP0/CPU0:router(config)# RP/0/RP0/CPU0:router(config-pim-default-ipv64)#</td>
<td></td>
</tr>
<tr>
<td>Step 3 rpf topology route-policy policy-name</td>
<td>Assigns a given routing policy to an RPF topology table.</td>
</tr>
<tr>
<td>Example: RP/0/RP0/CPU0:router(config-pim-default-ipv4)# rpf topology route-policy mtpolicy</td>
<td></td>
</tr>
<tr>
<td>Step 4 exit</td>
<td>Exits pim address-family configuration submode and returns you to global configuration mode.</td>
</tr>
<tr>
<td>Example: RP/0/RP0/CPU0:router(config-pim-default-ipv64)# exit RP/0/RP0/CPU0:router(config)#</td>
<td></td>
</tr>
</tbody>
</table>
Configuring MVPN Extranet Routing

To be able to import unicast routes from source VRFs to receiver VRFs, the import route targets of receiver VRFs must match the export route targets of a source VRF. Also, all VRFs on the PEs where the extranet source-receiver switchover takes place should be added to the BGP router configuration on those PEs.

Configuring MVPN extranet routing consists of these mandatory and optional tasks, which should be performed in the sequence shown:

- Configuring VPN Route Targets, page MCC-53 (required)

### Command or Action

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>`multicast-routing address-family {ipv4</td>
<td>ipv6}`</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> RP/0/RP0/CPU0::router(config)# multicast-routing address-family ipv4</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td><code>interface all enable</code></td>
<td>Enables multicast routing and forwarding on all new and existing interfaces.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> RP/0/RP0/CPU0::router(config-mcast-default-ipv4)# interface all enable</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td><code>end</code> or <code>commit</code></td>
<td>Saves configuration changes.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> RP/0/RP0/CPU0::router(config-mcast-default-ipv4) # end or RP/0/RP0/CPU0::router(config-mcast-default-ipv4) # commit</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>`show pim [vrf vrf-name] [ipv4</td>
<td>ipv6] [((unicast</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> RP/0/RP0/CPU0::router# show pim vrf mtt rpf ipv4 multicast topology all rpf</td>
<td></td>
</tr>
</tbody>
</table>
Implementing Multicast Routing on Cisco IOS XR Software

How to Implement Multicast Routing

- Enabling a VPN for Multicast Routing, page MCC-43 (required)
- “Configuring a Routing Policy” (required only if performing the following task)
  For information, see Cisco IOS XR Routing Configuration Guide.
- “Configuring an RPF Topology in PIM” section on page MCC-51 (optional)
  For more information about MVPN extranet routing, see MVPN IPv4 and IPv6 Connectivity, page MCC-15. For examples of an end-to-end configuration of each of the two available MVPN extranet topology solutions, see Configuring MVPN Extranet Routing: Example, page MCC-85.

Prerequisites for MVPN Extranet Routing

- PIM-SM and PIM-SSM are supported. You must configure the multicast group range in the source and receiver VRFs with a matching PIM mode.
- Because only static RP configuration is currently supported for a given multicast group range, both source and receiver MVPFs must be configured with the same RP.
- In the MVPN IPv4 and IPv6 Connectivity, page MCC-15 topology model, the data MDT encapsulation range should be large enough to accommodate extranet streams without any aggregation. This prevents extranet traffic, flowing to multiple VRFs, from being carried into only one data MDT.
- Data MDT configuration is required on only the Source VRF and Source PE Router.

Restrictions for MVPN Extranet Routing

- PIM-DM and PIM-BIDIR are not supported.
- Cisco IOS XR software supports only IPv4 extranet multicast routing over IPv4 core multicast routing.
- Any PE can be configured as an RP except a PE in the “Receiver VRF on the Source PE Router” model where the extranet switchover occurs, and where the source VRF has no interfaces. This is because the source VRF must have some physical interface to signal the data packets being received from the first hop.
- Cisco IOS XR currently supports only one encapsulation of VRF traffic on an extranet. This means that only one encapsulation interface (or MDT) is allowed in the outgoing forwarding interface list of the multicast route. If, for a given stream, there are multiple receiver VRFs joining the same source VRF, only the first receiver VRF receives traffic; other receiver VRF joins are discarded.

Note: This limitation applies to only the topology model MVPN IPv4 and IPv6 Connectivity, page MCC-15.

Configuring VPN Route Targets

This procedure demonstrates how to configure a VPN route target for each topology.

Note: Route targets should be configured so that the receiver VRF has unicast reachability to prefixes in the source VRF. These configuration steps can be skipped if prefixes in the source VRF are already imported to the receiver VRF.
SUMMARY STEPS

1. configure
2. vrf source-vrf
3. address-family {ipv4 | ipv6} unicast

Note
Only IPv4 addressing is currently supported for extranet.

4. import route-target [xx.yy:nn | as-number:nn | ip-address:nn]
5. export route-target [xx.yy:nn | as-number:nn | ip-address:nn]
6. end or commit
7. configure
8. vrf receiver-vrf

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure</td>
</tr>
<tr>
<td>Example:</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
| ```
RP/0/RP0/CPU0:router# configure
``` |
| **Step 2**        | vrf source-vrf |
| Example:          | Configures a VRF instance for the source PE router. |
| ```
RP/0/RP0/CPU0:router(config)# vrf green
RP/0/RP0/CPU0:router(config-vrf)#
``` |
| **Step 3**        | address-family {ipv4 | ipv6} unicast |
| Example:          | Specifies a unicast IPv4 or IPv6 address family and enters address family configuration submode. |
| ```
RP/0/RP0/CPU0:router(config-vrf)#
address-family ipv4 unicast
``` |
| **Step 4**        | import route-target [xx.yy:nn | as-number:nn | ip-address:nn] |
| Example:          | Imports the selected route target, optionally expressed as one of the following:
- 4-byte AS number of the route target in xx.yy:nn format. Range is 0-65535.0-65535:0-65535
- AS number of the route target in nn format. Range is 0-65535.
- IP address of the route target in A.B.C.D. format. |
| ```
RP/0/RP0/CPU0:router(config-vrf-af)# import route-target 234:222
``` |
| ```
RP/0/CPU0:router(config-vrf-af)# import route-target 100:100
``` |
Interconnecting PIM-SM Domains with MSDP

To set up an MSDP peering relationship with MSDP-enabled routers in another domain, you configure an MSDP peer to the local router.

If you do not want to have or cannot have a BGP peer in your domain, you could define a default MSDP peer from which to accept all Source-Active (SA) messages.

Finally, you can change the Originator ID when you configure a logical RP on multiple routers in an MSDP mesh group.
Prerequisites for Interconnecting PIM-SM Domains with MSDP

You must configure MSDP default peering, if the addresses of all MSDP peers are not known in BGP or multiprotocol BGP.

SUMMARY STEPS

1. configure
2. interface type interface-path-id
3. ipv4 address address mask
4. end
5. router msdp
6. default-peer ip-address [prefix-list list]
7. originator-id type interface-path-id
8. peer peer-address
9. connect-source type interface-path-id
10. mesh-group name
11. remote-as as-number
12. end or commit
13. show msdp [ipv4] globals
14. show msdp [ipv4] peer [peer-address]
15. show msdp [ipv4] rpf rpf-address

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RP0/CPU0:router# configure</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>interface type interface-path-id (Optional) Enters interface configuration mode to define the IPv4 address for the interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RP0/CPU0:router(config)# interface loopback 0 Note This step is required if you specify an interface type and number whose primary address becomes the source IP address for the TCP connection.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>ipv4 address address mask (Optional) Defines the IPv4 address for the interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RP0/CPU0:router(config-if)# ipv4 address 10.0.1.3 255.255.255.0 Note This step is required only if you specify an interface type and number whose primary address becomes the source IP address for the TCP connection. See optional for information about configuring the connect-source command.</td>
</tr>
</tbody>
</table>
### How to Implement Multicast Routing

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong></td>
<td>exit</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RP0/CPU0:router(config-if)# end</td>
</tr>
<tr>
<td><strong>Purpose</strong></td>
<td>Exits interface configuration mode, and returns the router to global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>router msdp</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RP0/CPU0:router(config)# router msdp</td>
</tr>
<tr>
<td><strong>Purpose</strong></td>
<td>Enters MSDP protocol configuration mode.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>default-peer ip-address [prefix-list list]</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RP0/CPU0:router(config-msdp)# default-peer 172.23.16.0</td>
</tr>
<tr>
<td><strong>Purpose</strong></td>
<td>(Optional) Defines a default peer from which to accept all MSDP SA messages.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>originator-id type interface-path-id</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RP0/CPU0:router(config-msdp)# originator-id pos 0/1/1/0</td>
</tr>
<tr>
<td><strong>Purpose</strong></td>
<td>(Optional) Allows an MSDP speaker that originates a (Source-Active) SA message to use the IP address of the interface as the RP address in the SA message.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>peer peer-address</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RP0/CPU0:router(config-msdp)# peer 172.31.1.2</td>
</tr>
<tr>
<td><strong>Purpose</strong></td>
<td>Enters MSDP peer configuration mode and configures an MSDP peer.</td>
</tr>
<tr>
<td>- Configure the router as a BGP neighbor.</td>
<td></td>
</tr>
<tr>
<td>- If you are also BGP peering with this MSDP peer, use the same IP address for MSDP and BGP. You are not required to run BGP or multiprotocol BGP with the MSDP peer, as long as there is a BGP or multiprotocol BGP path between the MSDP peers.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>connect-source type interface-path-id</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RP0/CPU0:router(config-msdp-peer)# connect-source loopback 0</td>
</tr>
<tr>
<td><strong>Purpose</strong></td>
<td>(Optional) Configures a source address used for an MSDP connection.</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>mesh-group name</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RP0/CPU0:router(config-msdp-peer)# mesh-group internal</td>
</tr>
<tr>
<td><strong>Purpose</strong></td>
<td>(Optional) Configures an MSDP peer to be a member of a mesh group.</td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td>remote-as as-number</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RP0/CPU0:router(config-msdp-peer)# remote-as 250</td>
</tr>
<tr>
<td><strong>Purpose</strong></td>
<td>(Optional) Configures the remote autonomous system number of this peer.</td>
</tr>
</tbody>
</table>
Controlling Source Information on MSDP Peer Routers

Your MSDP peer router can be customized to control source information that is originated, forwarded, received, cached, and encapsulated.

When originating Source-Active (SA) messages, you can control to whom you will originate source information, based on the source that is requesting information.

When forwarding SA messages you can do the following:
- Filter all source/group pairs
- Specify an extended access list to pass only certain source/group pairs
- Filter based on match criteria in a route map

When receiving SA messages you can do the following:
- Filter all incoming SA messages from an MSDP peer

### Command or Action | Purpose
--- | ---
**Step 12**  
end  
or  
commit | Saves configuration changes.  
- When you issue the end command, the system prompts you to commit changes:  
  Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:  
  - Entering yes saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.  
  - Entering no exits the configuration session and returns the router to EXEC mode without committing the configuration changes.  
  - Entering cancel leaves the router in the current configuration session without exiting or committing the configuration changes.  
  - Use the commit command to save the configuration changes to the running configuration file and remain within the configuration session.

**Step 13**  
show msdp [ipv4] globals | Displays the MSDP global variables.

**Step 14**  

**Step 15**  
show msdp [ipv4] rpf rpf-address | Displays the RPF lookup.
- Specify an extended access list to pass certain source/group pairs
- Filter based on match criteria in a route map

In addition, you can use time to live (TTL) to control what data is encapsulated in the first SA message for every source. For example, you could limit internal traffic to a TTL of eight hops. If you want other groups to go to external locations, you send those packets with a TTL greater than eight hops.

By default, MSDP automatically sends SA messages to peers when a new member joins a group and wants to receive multicast traffic. You are no longer required to configure an SA request to a specified MSDP peer.

**SUMMARY STEPS**

1. configure
2. router msdp
3. sa-filter {in | out} {ip-address | peer-name} [list access-list-name] [rp-list access-list-name]
4. cache-sa-state [list access-list-name] [rp-list access-list-name]
5. ttl-threshold ttl-value
6. exit
7. ipv4 access-list name [sequence-number] permit any source [source-wildcard]
8. end or commit

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RP0/CPU0:router# configure</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> router msdp</td>
<td>Enters MSDP protocol configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RP0/CPU0:router(config)# router msdp</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> sa-filter {in</td>
<td>out} {ip-address</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RP0/CPU0:router(config-msdp)# sa-filter out router.cisco.com list 100</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If you specify both the list and rp-list keywords, all conditions must be true to pass any source, group (S, G) pairs in outgoing Source-Active (SA) messages.</td>
</tr>
<tr>
<td></td>
<td>• You must configure the ipv4 access-list command in Step 7.</td>
</tr>
<tr>
<td></td>
<td>• If all match criteria are true, a permit from the route map passes routes through the filter. A deny filters routes.</td>
</tr>
<tr>
<td></td>
<td>• This example allows only (S, G) pairs that pass access list 100 to be forwarded in an SA message to the peer named router.cisco.com.</td>
</tr>
</tbody>
</table>
### Command or Action

#### Step 4
**cache-sa-state** \([list\ access-list-name] [rp-list\ access-list-name]\)

**Example:**
RP/0/RP0/CPU0:router(config-msdp)#
cache-sa-state 100

- *Purpose*
  - Creates and caches source/group pairs from received Source-Active (SA) messages and controls pairs through access lists.

#### Step 5
**ttl-threshold** \(ttl-value\)

**Example:**
RP/0/RP0/CPU0:router(config-msdp)#
ttl-threshold 8

- *Purpose*
  - (Optional) Limits which multicast data is sent in SA messages to an MSDP peer.
    - Only multicast packets with an IP header TTL greater than or equal to the \(ttl-value\) argument are sent to the MSDP peer specified by the IP address or name.
    - Use this command if you want to use TTL to examine your multicast data traffic. For example, you could limit internal traffic to a TTL of 8. If you want other groups to go to external locations, send those packets with a TTL greater than 8.
    - This example configures a TTL threshold of eight hops.

#### Step 6
**exit**

**Example:**
RP/0/RP0/CPU0:router(config-msdp)# exit

- *Purpose*
  - Exits the current configuration mode.
### Implementing Multicast Routing on Cisco IOS XR Software

#### How to Implement Multicast Routing

**MCC-61**

**OL-24702-01**

### Configuring MSDP MD5 Password Authentication

#### SUMMARY STEPS

1. configure
2. router msdp
3. peer peer-address
4. password [clear | encrypted] password
5. end or commit
6. show mfib [vrf vrf-name] [ipv4 | ipv6] hardware route [*/source-address | group-address [prefix-length]] location node-id

---

**Command or Action**

**Step 7**

`ipv4 access-list name [sequence-number] permit any source [source-wildcard]`

**Example:**

RP/0/RP0/CPU0:router(config)# ipv4 access-list 100 20 permit any 239.1.1.1 0.0.0.0

**Purpose**

- Defines an IPv4 access list to be used by SA filtering.
- In this example, the access list 100 permits multicast group 239.1.1.1.
- The `ipv4 access-list` command is required if the keyword **list** is configured for SA filtering in **Step 3**.

**Note**

- There must be one “any” in order to successfully commit the [group-access-list]. Deny statements are ignored.

**Step 8**

`end`

or

`commit`

**Example:**

RP/0/RP0/CPU0:router(config-ipv4-acl)# end

or

RP/0/RP0/CPU0:router(config-ipv4-acl)# commit

**Purpose**

- Saves configuration changes.
- When you issue the `end` command, the system prompts you to commit changes:

  `Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`

  - Entering `yes` saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
  - Entering `no` exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
  - Entering `cancel` leaves the router in the current configuration session without exiting or committing the configuration changes.

- Use the `commit` command to save the configuration changes to the running configuration file and remain within the configuration session.

---

**Command or Action**

**Step 7**

`ipv4 access-list name [sequence-number] permit any source [source-wildcard]`

**Example:**

RP/0/RP0/CPU0:router(config)# ipv4 access-list 100 20 permit any 239.1.1.1 0.0.0.0

**Purpose**

- Defines an IPv4 access list to be used by SA filtering.
- In this example, the access list 100 permits multicast group 239.1.1.1.
- The `ipv4 access-list` command is required if the keyword **list** is configured for SA filtering in **Step 3**.

**Note**

- There must be one “any” in order to successfully commit the [group-access-list]. Deny statements are ignored.

**Step 8**

`end`

or

`commit`

**Example:**

RP/0/RP0/CPU0:router(config-ipv4-acl)# end

or

RP/0/RP0/CPU0:router(config-ipv4-acl)# commit

**Purpose**

- Saves configuration changes.
- When you issue the `end` command, the system prompts you to commit changes:

  `Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`

  - Entering `yes` saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
  - Entering `no` exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
  - Entering `cancel` leaves the router in the current configuration session without exiting or committing the configuration changes.

- Use the `commit` command to save the configuration changes to the running configuration file and remain within the configuration session.

---

**Configuring MSDP MD5 Password Authentication**

**SUMMARY STEPS**

1. configure
2. router msdp
3. peer peer-address
4. password [clear | encrypted] password
5. end or commit
6. show mfib [vrf vrf-name] [ipv4 | ipv6] hardware route [*/source-address | group-address [prefix-length]] location node-id
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>RP/0/RP0/CPU0:router# configure</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> router msdp</td>
<td>Enters MSDP configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>RP/0/RP0/CPU0:router(config)# router msdp</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> peer peer-address</td>
<td>Configures the MSDP peer.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>RP/0/RP0/CPU0:router(config-msdp)# peer 10.0.5.4</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> password {clear</td>
<td>encrypted} password</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>RP/0/RP0/CPU0:router(config-msdp-peer)# password encrypted a34bi5m</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> end or commit</td>
<td>Saves configuration changes.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>RP/0/RP0/CPU0:router(config-msdp-peer)# end</td>
<td></td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td>RP/0/RP0/CPU0:router(config-msdp-peer)# commit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> show mfib [vrf vrf-name] [ipv4</td>
<td>ipv6] hardware route (*</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>RP/0/RP0/CPU0:router# show mfib hardware route</td>
<td></td>
</tr>
<tr>
<td>* location 0/1/cpu0</td>
<td></td>
</tr>
</tbody>
</table>
Multicast only fast reroute (MoFRR)

MoFRR allows fast reroute for multicast traffic on a multicast router. MoFRR minimizes packet loss in a network when node or link failures occur (at the topology merge point). It works by making simple enhancements to multicast routing protocols.

MoFRR involves transmitting a multicast join message from a receiver towards a source on a primary path and transmitting a secondary multicast join message from the receiver towards the source on a backup path. Data packets are received from the primary and secondary paths. The redundant packets are discarded at topology merge points with the help of Reverse Path Forwarding (RPF) checks. When a failure is detected on the primary path, the repair occurs locally by changing the interface on which packets are accepted to the secondary interface, thus improving the convergence times in the event of a node or link failure on the primary path.

Currently MoFRR is supported on Equal Cost MultiPath (ECMP) topologies only. XML support is available for MoFRR.

Operating Modes of MoFRR

- RIB-based MoFRR—Supports Cisco CRS and XR12000 series routers; the RIB version is configured at the software level and is based on routing convergence. RIB events are used as trigger for switchover.
- Flow-based MoFRR—Supports the Cisco ASR 9000 Series Aggregation Services Router. Flow-based exposes the primary and secondary RPF interfaces to the forwarding plane, with switchover occurring entirely at the hardware level.

Faster convergence is obtainable in Flow-based MoFRR by monitoring the packet counts of the primary stream. If no activity is detected for 30 ms, the switch over is triggered to the backup stream and the traffic loss is within 50 ms.

Restrictions

These limitations apply to MoFRR deployments when the Cisco ASR 9000 Series SPA Interface Processor-700 linecard is used in the Cisco ASR 9000 Series Router chassis.

1. Cisco ASR 9000 Series SPA Interface Processor-700 cannot be used on ingress interface as either the primary or backup (ECMP paths) path back to the multicast source.
2. The egress interfaces on Cisco ASR 9000 Series SPA Interface Processor-700 may lead to duplicate multicast streams for short periods of time (the time between the switch from Trident primary to Trident backup paths on ingress).

Configuring MoFRR

RIB-based MoFRR

SUMMARY STEPS

1. configure
2. router pim
Implementing Multicast Routing on Cisco IOS XR Software

Point-to-Multipoint Traffic Engineering Label-Switched Multicast

IP multicast was traditionally used for IPTV broadcasting and content delivery services. MPLS-TE (traffic engineering) is fast replacing the IP multicast technique because of the various advantages of MPLS-TE, such as:

- Fast re-routing and restoration in case of link/ node failure
- Bandwidth guarantee
- Explicit path setting along with off-line computation

MPLS supports point-to-point path. However, in order to use MPLS for multicast service, MPLS has to be extended to handle point-to-multipoint paths. A reliable solution to signal Point-to-Multipoint (P2MP) label switched paths(LSP) is the Point-to-Multipoint TE LSP. This solution uses the Resource Reservation Protocol- Traffic Engineering (RSVP-TE) extension as the signaling protocol for establishing P2MP TE LSPs.

Point to Multipoint LSP(P2MP)

P2MP LSP is unidirectional. In case of native IP multicast, the multicast forwarding always has to perform an acceptance check. This check ensures all multicast packets undergo a RPF check to ensure that the packets have arrived on the correct interface in the direction of the source. However, the acceptance check with MPLS forwarding may be different in case of an unicast or upstream label.

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>RP/0/RP0/CPU0:router# configure</td>
<td></td>
</tr>
<tr>
<td>Step 2 router pim</td>
<td>Enters the PIM configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>RP/0/RP0/CPU0:router(config)# router pim</td>
<td></td>
</tr>
<tr>
<td>Step 3 mofrr rib acl-name</td>
<td>Enter the ACL name.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>RP/0/RP0/CPU0:router(pim)# mofrr rib acl1</td>
<td></td>
</tr>
<tr>
<td>Step 4 end or commit class-map</td>
<td>Saves the configuration changes.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>RP/0/RP0/CPU0:router(pim)# commit</td>
<td></td>
</tr>
</tbody>
</table>
Depending on the multicast signaling protocol, the labeled packet may require an additional L3 lookup at the P and PE routers in order to forward the multicast packet to the physical interfaces according to multicast routing. In this case, the incoming P2MP LSP as the incoming interface for the received multicast packet must also be available to the multicast forwarding plane during the L3 lookup. For more details on RSVP-TE and P2MP LSP, refer the Cisco IOS XR MPLS Configuration Guide for the CRS Router.

**Label Switched Multicast (LSM) Multicast Label Distribution Protocol (mLDP) based Multicast VPN (mVPN) Support**

Label Switch Multicast (LSM) is MPLS technology extensions to support multicast using label encapsulation. CRS next generation MVPN is based on Multicast Label Distribution Protocol (mLDP), which can be used to build P2MP and MP2MP LSPs through a MPLS network. These LSPs can be used for transporting both IPv4 and IPv6 multicast packets, either in the global table or VPN context. mLDP is complementary to the Cisco LSM strategy.

**Multicast Routing Protocol support for P2MP**

All multicast routing protocols support P2MP TE LSP. At ingress node, a multicast protocol must make a mapping between the multicast traffic and the P2MP TE LSP with the configuration of static-join. At egress node, the multicast protocol must conduct a special RPF check for the multicast packet which is received from MPLS core and forward it to the customer facing interface. The RPF check is based on the configuration of static-rpf. These multicast groups which are forwarded over the P2MP TE LSPs can be specified with the static-rpf configuration in case of PIM-SSM.

**Enabling Multicast Forwarding over tunnel interface (at ingress node)**

This configuration is used for allowing the forwarding of the multicast packet over the specified interface.

**SUMMARY STEPS**

1. configure
2. multicast-routing
3. address-family {ipv4 | ipv6}
4. interface tunnel-mte range
5. enable | disable
6. end or commit
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RP0/CPU0:router# configure</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> multicast-routing</td>
<td>Enters multicast routing configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RP0/CPU0:router(config)# multicast-routing</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> address-family {ipv4</td>
<td>ipv6}</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RP0/CPU0:router(config-mcast)# address-family ipv4</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> interface tunnel-mte range</td>
<td>Specify the range. The range is 0 to 65535.</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RP0/CPU0:router(config-mcast-default-ipv4)# interface tunnel-mte 100</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> enable</td>
<td>If enable is set, MFIB forwards multicast packets over the interface.</td>
</tr>
<tr>
<td><strong>Step 5</strong> disable</td>
<td>If disable is set, MFIB stops forwarding multicast packets over the interface.</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RP0/CPU0:router(config-mcast-default-ipv4)# enable</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RP0/CPU0:router(config-mcast-default-ipv4)# disable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> end</td>
<td>Saves configuration changes.</td>
</tr>
<tr>
<td><strong>Step 6</strong> or commit</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RP0/CPU0:router(config-mcast-default-ipv4)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RP0/CPU0:router(config-mcast-default-ipv4)# commit</td>
<td></td>
</tr>
</tbody>
</table>

- When you issue the **end** command, the system prompts you to commit changes:

  Uncommitted changes found, commit them before exiting (yes/no/cancel)? [cancel]:

  - Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
  - Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
  - Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.

- Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.
# P2MP configurations at egress node and bud node

## Configuring Static Reverse Path Forwarding (RPF)

### SUMMARY STEPS

1. `configure`
2. `multicast-routing`
3. `address-family {ipv4 | ipv6}`
4. `static-rpf address range prefix`
5. `mpls address`
6. `end` or `commit`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RP0/CPU0:router# configure</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters multicast routing configuration mode.</td>
</tr>
<tr>
<td><code>multicast-routing</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RP0/CPU0:router(config)# multicast-routing</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Enters ipv4 (or ipv6) address-family submode.</td>
</tr>
<tr>
<td>`address-family {ipv4</td>
<td>ipv6}`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RP0/CPU0:router(config-mcast)# address-family ipv4</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Enter the source and prefix length.</td>
</tr>
<tr>
<td><code>static-rpf address range prefix</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RP0/CPU0:router(config-mcast-default-ipv4)# static-rpf 10.1.1.1 32</td>
</tr>
</tbody>
</table>
**Configuring core tree protocol**

**SUMMARY STEPS**

1. configure  
2. multicast-routing  
3. address-family \{ipv4 | ipv6\}  
4. core-tree-protocol rsvp-te group-list \textit{name}  
5. end or commit
# DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure</strong>&lt;br&gt;Example:&lt;br&gt;RP/0/RP0/CPU0:router# configure</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>multicast-routing</strong>&lt;br&gt;Example:&lt;br&gt;RP/0/RP0/CPU0:router(config)# multicast-routing</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>**address-family (ipv4</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>core-tree-protocol rsvp-te group-list name</strong>&lt;br&gt;Example:&lt;br&gt;RP/0/RP0/CPU0:router(config-mcast-default-ipv4) # core-tree-protocol rsvp-te group-list acl1</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>end</strong>&lt;br&gt;<strong>commit</strong>&lt;br&gt;Example:&lt;br&gt;RP/0/RP0/CPU0:router(config-mcast-default-ipv4) # end&lt;br&gt;or&lt;br&gt;RP/0/RP0/CPU0:router(config-mcast-default-ipv4) # commit</td>
</tr>
</tbody>
</table>
Configuration Examples for Implementing Multicast Routing on Cisco IOS XR Software

This section provides the following configuration examples:
- MSDP Anycast RP Configuration on Cisco IOS XR Software: Example, page MCC-70
- Bidir-PIM Configuration on Cisco IOS XR Software: Example, page MCC-71
- Calculating Rates per Route: Example, page MCC-72
- Preventing Auto-RP Messages from Being Forwarded on Cisco IOS XR Software: Example, page MCC-73
- Inheritance in MSDP on Cisco IOS XR Software: Example, page MCC-73
- Configuring IPv4 Multicast VPN: Example, page MCC-74
- Configuring Multitopology Routing: Example, page MCC-84
- Configuring MVPN Extranet Routing: Example, page MCC-85
- Configuring Multicast Hub and Spoke Topology: Example, page MCC-90

MSDP Anycast RP Configuration on Cisco IOS XR Software: Example

Anycast RP allows two or more rendezvous points (RPs) to share the load for source registration and to act as hot backup routers for each other. MSDP is the key protocol that makes Anycast RP possible.

In Anycast RP, two or more RPs are configured with the same IP address on loopback interfaces. Configure the Anycast RP loopback address with a 32-bit mask, making it a host address. Configure all downstream routers to “know” that the Anycast RP loopback address is the IP address of the local RP. IP routing automatically selects the topologically closest RP for each source and receiver.

As a source may register with one RP and receivers may join to a different RP, a method is needed for the RPs to exchange information about active sources. This information exchange is done with MSDP.

In Anycast RP, all the RPs are configured to be MSDP peers of each other. When a source registers with one RP, a Source-Active (SA) message is sent to the other RPs, informing them that there is an active source for a particular multicast group. The result is that each RP knows about the active sources in the area of the other RPs. If any of the RPs fails, IP routing converges and one of the RPs becomes the active RP in more than one area. New sources register with the backup RP, and receivers join the new RP.

Note that the RP is usually needed only to start new sessions with sources and receivers. The RP facilitates the shared tree so that sources and receivers can directly establish a multicast data flow. If a multicast data flow is already directly established between a source and the receiver, an RP failure does not affect that session. Anycast RP ensures that new sessions with sources and receivers can begin at any time.

The following Anycast RP example configures Router A and Router B as Anycast RPs. The Anycast RP IP address assignment is 10.0.0.1.

**Router A**

```
interface loopback 0
ipv4 address 10.0.0.1/32
no shutdown
interface loopback 1
ipv4 address 10.2.0.1/32
no shutdown
```

multicast-routing
  interfaces all enable
router pim
  rp-address 10.0.0.1
router msdp
  connect-source loopback 1
  peer 10.2.0.2

Router B
interface loopback 0
  ipv4 address 10.0.0.1/32
  no shutdown
interface loopback 1
  ipv4 address 10.2.0.2/32
  no shutdown
multicast-routing
  interfaces all enable
router pim
  rp-address 10.0.0.1
router msdp
  connect-source loopback 1
  peer 10.2.0.1

Apply the following configuration to all network routers:

  multicast-routing
  router pim
  rp-address 10.0.0.1

Bidir-PIM Configuration on Cisco IOS XR Software: Example

An access list on the RP can be used to specify a list of groups to be advertised as bidirectional PIM (bidir-PIM).

The following example shows how to configure an RP for both PIM-SM and the bidir-PIM mode groups. The bidir-PIM groups are configured as 224/8 and 227/8, with the remaining multicast group range (224/4) configured as PIM-SM.

interface loopback 0
  ipv4 address 10.0.0.1/24
  no shutdown
interface loopback 1
  ipv4 address 10.2.0.1/24
  no shutdown
ipv4 access-list bidir_acl
  10 permit 224.0.0.0 0.255.255.255 any
  20 permit 225.0.0.0 0.255.255.255 any
multicast-routing
  interfaces all enable
router pim
  auto-rp mapping-agent loopback 0 scope 15 interval 60
  auto-rp candidate-rp loopback 0 scope 15 group-list bidir_acl interval 60 bidir
  auto-rp candidate-rp loopback 1 scope 15 group-list 224/4 interval 60

Tip

Issue the show pim group-map command and verify the output to ensure that the configured mappings are learned correctly.
Calculating Rates per Route: Example

The following example illustrates output from hardware counters based on rate per route for a specific source and group address location:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# multicast-routing vrf vpn12 address-family ipv4
RP/0/RP0/CPU0:router(config-mcast-default-ipv4)# rate-per-route
RP/0/RP0/CPU0:router(config-mcast-default-ipv4)# interface all enable
RP/0/RP0/CPU0:router(config-mcast-default-ipv4)# accounting per-prefix
RP/0/RP0/CPU0:router(config-mcast-default-ipv4)# commit
RP/0/RP0/CPU0:router(config-mcast-default-ipv4)# exit
RP/0/RP0/CPU0:router(config)# exit
RP/0/RP0/CPU0:router# show mfib route rate

IP Multicast Forwarding Rates Source Address, Group Address HW Forwarding Rates: bps In/pps In/bps Out/ppps Out

<table>
<thead>
<tr>
<th>Source Address</th>
<th>bps_in</th>
<th>pps_in</th>
<th>bps_out</th>
<th>pps_out</th>
</tr>
</thead>
<tbody>
<tr>
<td>(*,224.0.0.0/24)</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>(*,224.0.1.39)</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>(*,224.0.1.40)</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>(*,232.0.0.0/8)</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>(30.0.70.2,225.0.0.0)</td>
<td>22649</td>
<td>50</td>
<td>22951</td>
<td>50</td>
</tr>
<tr>
<td>(30.0.70.2,225.0.0.1)</td>
<td>22649</td>
<td>50</td>
<td>22951</td>
<td>50</td>
</tr>
<tr>
<td>(30.0.70.2,225.0.0.2)</td>
<td>22649</td>
<td>50</td>
<td>22951</td>
<td>50</td>
</tr>
<tr>
<td>(30.0.70.2,225.0.0.3)</td>
<td>22649</td>
<td>50</td>
<td>22951</td>
<td>50</td>
</tr>
<tr>
<td>(30.0.70.2,225.0.0.4)</td>
<td>22649</td>
<td>50</td>
<td>22951</td>
<td>50</td>
</tr>
<tr>
<td>(30.0.70.2,225.0.0.5)</td>
<td>22649</td>
<td>50</td>
<td>22951</td>
<td>50</td>
</tr>
<tr>
<td>(30.0.70.2,225.0.0.6)</td>
<td>22649</td>
<td>50</td>
<td>22951</td>
<td>50</td>
</tr>
</tbody>
</table>
```
Preventing Auto-RP Messages from Being Forwarded on Cisco IOS XR Software: Example

This example shows that Auto-RP messages are prevented from being sent out of the Packet over SONET/SDH (POS) interface 0/3/0/0. It also shows that access list 111 is used by the Auto-RP candidate and access list 222 is used by the boundary command to contain traffic on POS interface 0/3/0/0.

```cisco
ipv4 access-list 111
  10 permit 224.1.0.0 0.0.255.255 any
  20 permit 224.2.0.0 0.0.255.255 any
!
!Access list 111 is used by the Auto-RP candidate.
!
ipv4 access-list 222
  10 deny any host 224.0.1.39
  20 deny any host 224.0.1.40
!
!Access list 222 is used by the boundary command to contain traffic (on POS0/3/0/0) that is sent to groups 224.0.1.39 and 224.0.1.40.
!
router pim
  auto-rp mapping-agent loopback 2 scope 32 interval 30
  auto-rp candidate-rp loopback 2 scope 15 group-list 111 interval 30
multicast-routing
  interface pos 0/3/0/0
  boundary 222
```

Inheritance in MSDP on Cisco IOS XR Software: Example

The following MSDP commands can be inherited by all MSDP peers when configured under router MSDP configuration mode. In addition, commands can be configured under the peer configuration mode for specific peers to override the inheritance feature.

- **connect-source**
- **sa-filter**
- **ttl-threshold**

If a command is configured in both the router msdp and peer configuration modes, the peer configuration takes precedence.

In the following example, MSDP on Router A filters Source-Active (SA) announcements on all peer groups in the address range 226/8 (except IP address 172.16.0.2); and filters SAs sourced by the originator RP 172.16.0.3 to 172.16.0.2.

MSDP peers (172.16.0.1, 172.16.0.2, and 172.17.0.1) use the loopback 0 address of Router A to set up peering. However, peer 192.168.12.2 uses the IPv4 address configured on the Packet-over-SONET/SDH (POS) interface to peer with Router A.

**Router A**

```cisco
! ipv4 access-list 111
  10 deny ip host 172.16.0.3 any
  20 permit any any
!
ipv4 access-list 112
```

OL-24702-01

Cisco ASR 9000 Series Aggregation Services Router Multicast Configuration Guide

MCC-73
Implementing Multicast Routing on Cisco IOS XR Software

Configuration Examples for Implementing Multicast Routing on Cisco IOS XR Software

MCC-74
Cisco ASR 9000 Series Aggregation Services Router Multicast Configuration Guide
OL-24702-01

```
10 deny any 226.0.0.0 0.255.255.255
30 permit any any
!
router msdp
    connect-source loopback 0
    sa-filter in rp-list 111
    sa-filter out rp-list 111
    peer 172.16.0.1
        !
    peer 172.16.0.2
        sa-filter out list 112
        !
    peer 172.17.0.1
        !
    peer 192.168.12.2
        connect-source pos 0/2/0/0
        !
```

Configuring IPv4 Multicast VPN: Example

Cisco CRS Router supports only IPv4 addressing.

This end-to-end configuration example shows how to establish a multicast VPN topology (Figure 9), using two different routing protocols (OSPF or BGP) to broadcasting traffic between customer-edge (CE) routers and provider-edge (PE) routers:

- Configuring MVPN to Advertise Routes Between the CE and the PE Using OSPF: Example, page MCC-74
- Configuring MVPN to Advertise Routes Between the CE and the PE Using BGP: Example, page MCC-79

![Topology in MVPN Configuration](image)

For more configuration information, see the “Configuring Multicast VPN” section on page MCC-41 of this module and also related configuration information in Cisco IOS XR Routing Configuration Guide.

Configuring MVPN to Advertise Routes Between the CE and the PE Using OSPF: Example

PE1:

```
!
vrf vpn1
    address-family ipv4 unicast
    import route-target
        1:1
        !
    export route-target
        1:1
        !
        !
```


interface Loopback0
  ipv4 address 1.1.1.1 255.255.255.255
!
interface Loopback1
  vrf vpn1
  ipv4 address 2.2.2.2 255.255.255.255
!
interface GigabitEthernet0/5/0/0
  vrf vpn1
  ipv4 address 101.1.1.1 255.255.255.0
!
interface TenGigE0/6/0/0
  ipv4 address 12.1.1.1 255.255.255.0
!
  mpls ldp
  router-id 1.1.1.1
!
interface TenGigE0/6/0/0
!
  multicast-routing
  vrf vpn1 address-family ipv4
    mdt data 233.1.0.0/16 threshold 3
    mdt default ipv4 232.1.1.1
    rate-per-route
    interface all enable accounting per-prefix
    !
    address-family ipv4
      nsf
      mdt source Loopback0
      interface all enable accounting per-prefix
    !
  !
  router bgp 100
  bgp router-id 1.1.1.1
  address-family ipv4 unicast
  !
  address-family vpnv4 unicast
  !
  address-family ipv4 mdt
  !
  neighbor 9.9.9.9
    remote-as 100
    update-source Loopback0
    address-family ipv4 unicast
    !
    address-family vpnv4 unicast
    !
    address-family ipv4 mdt
    !
  !
  vrf vpn1
  rd 1:1
  address-family ipv4 unicast
    redistribute ospf 1
    !
  !
  router ospf 1
  vrf vpn1
  router-id 2.2.2.2
  redistribute bgp 100
  area 0
interface Loopback1
!
interface GigabitEthernet0/5/0/0
!
!
router ospf 100
router-id 1.1.1.1
area 0
  interface Loopback0
  !
  interface TenGigE0/6/0/0
  !
  !
router pim vrf vpn1 address-family ipv4
  rp-address 2.2.2.2
  log neighbor changes
!
router pim vrf default address-family ipv4
  rp-address 1.1.1.1
!
end

PE2:
!
vrf vpn1
  address-family ipv4 unicast
  import route-target
  1:1
  !
  export route-target
  1:1
  !
  !
  interface Loopback0
  ipv4 address 9.9.9.9 255.255.255.255
  !
  interface Loopback1
  vrf vpn1
  ipv4 address 10.10.10.10 255.255.255.255
  !
  interface GigabitEthernet0/2/2/7
  vrf vpn1
  ipv4 address 122.1.1.1 255.255.255.0
  negotiation auto
  !
  interface TenGigE0/3/0/0
  ipv4 address 12.1.1.2 255.255.255.0
  !
mpls ldp
  router-id 9.9.9.9
  interface TenGigE0/3/0/0
  !
  !
multicast-routing
  vrf vpn1 address-family ipv4
  mdt data 233.1.0.0/16 threshold 3
  mdt default ipv4 232.1.1.1
  rate-per-route
  interface all enable
accounting per-prefix
!
address-family ipv4
 nsf
 mdt source Loopback0
 interface all enable
 accounting per-prefix
!
!
router bgp 100
 bgp router-id 9.9.9.9
 address-family ipv4 unicast
 !
 address-family vpnv4 unicast
 !
 address-family ipv4 mdt
 !
neighbor 1.1.1.1
 remote-as 100
 update-source Loopback0
 address-family ipv4 unicast
 !
 address-family vpnv4 unicast
 !
 address-family ipv4 mdt
 !
!
 vrf vpn1
 rd 1:1
 address-family ipv4 unicast
 redistribute ospf 1
 !
!
 router ospf 1
 vrf vpn1
 router-id 10.10.10.10
 redistribute bgp 100
 area 0
 interface Loopback1
 !
 interface GigabitEthernet0/2/2/7
 !
 !
 router ospf 100
 router-id 9.9.9.9
 area 0
 interface Loopback0
 !
 interface TenGigE0/3/0/0
 !
 !
 router pim vrf vpn1 address-family ipv4
 rp-address 2.2.2.2
 !
 router pim vrf default address-family ipv4
 rp-address 1.1.1.1
 !
end
CE4:

For information about configuring the CE router, using Cisco IOS software, see the appropriate Cisco IOS software configuration documentation.

! interface Loopback0
  ipv4 address 101.101.101.101 255.255.255.255
! interface GigabitEthernet0/0/0/0
  ipv4 address 101.1.1.2 255.255.255.0
! interface GigabitEthernet0/0/0/3
  ipv4 address 11.1.1.1 255.255.255.0
! multicast-routing
  address-family ipv4
    interface all enable
! router ospf 1
  router-id 101.101.101.101
  area 0
    interface Loopback0
    interface GigabitEthernet0/0/0/0
    interface GigabitEthernet0/0/0/3
! router pim vrf default address-family ipv4
  rp-address 2.2.2.2
    interface Loopback0
    interface GigabitEthernet0/0/0/0
    interface GigabitEthernet0/0/0/3
! end

CE3:

For information about configuring the CE router, using Cisco IOS software, see the appropriate Cisco IOS software configuration documentation.

interface Loopback0
  ipv4 address 122.122.122.122 255.255.255.255
!

interface GigabitEthernet0/1/3/0
  ipv4 address 22.1.1.1 255.255.255.0
!

interface GigabitEthernet0/2/3/0
  ipv4 address 122.1.1.2 255.255.255.0
!

multicast-routing
  address-family ipv4
    interface all enable
! router ospf 1
  router-id 122.122.122.122
  area 0
interface Loopback0

! interface GigabitEthernet0/1/3/0
! interface GigabitEthernet0/2/3/0
!
!
! router pim vrf default address-family ipv4
 rp-address 2.2.2.2
!
interface Loopback0
!
interface GigabitEthernet0/1/3/0
!
interface GigabitEthernet0/2/3/0
!
!
end

Configuring MVPN to Advertise Routes Between the CE and the PE Using BGP: Example

**PE1:**

vrf vpn1
address-family ipv4 unicast
    import route-target
  1:1
!
    export route-target
  1:1
!
!
interface Loopback0
 ipv4 address 1.1.1.1 255.255.255.255
!
interface Loopback1
 vrf vpn1
 ipv4 address 2.2.2.2 255.255.255.255
!
interface GigabitEthernet0/5/0/0
 vrf vpn1
 ipv4 address 101.1.1.1 255.255.255.0
!
interface TenGigE0/6/0/0
 ipv4 address 12.1.1.1 255.255.255.0
!
mpls ldp
 router-id 1.1.1.1
!
interface TenGigE0/6/0/0
!
!
multicast-routing
 vrf vpn1 address-family ipv4
 mdt data 233.1.0.0/16 threshold 3
 mdt default ipv4 232.1.1.1
 rate-per-route
 interface all enable
 accounting per-prefix
!
 address-family ipv4
 nsf
 mdt source Loopback0
interface all enable
  accounting per-prefix
!
!
  route-policy pass-all
    pass
end-policy
!
routerr bgp 100
  bgp router-id 1.1.1.1
  address-family ipv4 unicast
  !
  address-family vpv4 unicast
  !
  address-family ipv4 mdt
  !
neighbor 9.9.9.9
  remote-as 100
  update-source Loopback0
  address-family ipv4 unicast
  !
  address-family vpv4 unicast
  !
  address-family ipv4 mdt
  !
!
  vrf vpn1
  rd 1:1
  address-family ipv4 unicast
    redistribute connected
  !
neighbor 101.1.1.2
  remote-as 400
  address-family ipv4 unicast
    route-policy pass-all in
    route-policy pass-all out
  !
!
router ospf 100
  router-id 1.1.1.1
  area 0
    interface Loopback0
    !
    interface TenGigE0/6/0/0
    !
!
router pim vrf vpn1 address-family ipv4
  rp-address 2.2.2.2
  log neighbor changes
!
router pim vrf default address-family ipv4
  rp-address 1.1.1.1
!
end

PE2:
!
  vrf vpn1
address-family ipv4 unicast
  import route-target
  1:1
  !
export route-target
  1:1
  !
!
interface Loopback0
  ipv4 address 9.9.9.9 255.255.255.255
!
interface Loopback1
  vrf vpn1
  ipv4 address 10.10.10.10 255.255.255.255
!
interface GigabitEthernet0/2/2/7
  vrf vpn1
  ipv4 address 122.1.1.1 255.255.255.0
  negotiation auto
!
interface TenGigE0/3/0/0
  ipv4 address 12.1.1.2 255.255.255.0
!
mpls ldp
  router-id 9.9.9.9
  interface TenGigE0/3/0/0
  !
  !
  multicast-routing
  vrf vpn1 address-family ipv4
    mdt data 233.1.0.0/16 threshold 3
    mdt default ipv4 232.1.1.1
    rate-per-route
    interface all enable
    accounting per-prefix
    !
address-family ipv4
  nsf
  mdt source Loopback0
  interface all enable
  accounting per-prefix
  !
  !
route-policy pass-all
  pass
  end-policy
  !
router bgp 100
  bgp router-id 9.9.9.9
  address-family ipv4 unicast
  !
address-family vpnv4 unicast
  !
address-family ipv4 mdt
  !
neighbor 1.1.1.1
  remote-as 100
  update-source Loopback0
  address-family ipv4 unicast
  !
address-family vpnv4 unicast
  !
address-family ipv4 mdt
!
!
vrf vpn1
rd 1:1
address-family ipv4 unicast
  redistribute connected
!
neighbor 122.1.1.2
  remote-as 500
  address-family ipv4 unicast
    route-policy pass-all in
    route-policy pass-all out
!
!
router ospf 100
  router-id 9.9.9.9
  area 0
    interface Loopback0
    !
    interface TenGigE0/3/0/0
    !
  !
  router pim vrf vpn1 address-family ipv4
    rp-address 2.2.2.2
  !
  router pim vrf default address-family ipv4
    rp-address 1.1.1.1
  !
end

CE4:

For information about configuring the CE router, using Cisco IOS software, see the appropriate Cisco IOS software configuration documentation.

interface Loopback0
  ipv4 address 101.101.101.101 255.255.255.255
  !
interface GigabitEthernet0/0/0/0
  ipv4 address 101.1.1.2 255.255.255.0
  !
interface GigabitEthernet0/0/3
  ipv4 address 11.1.1.1 255.255.255.0
  !
multicast-routing
  address-family ipv4
    interface all enable
    !
    !
    route-policy pass-all
    pass
end-policy
!
router bgp 400
  bgp router-id 101.101.101.101
  address-family ipv4 unicast
  redistribute connected
  !
  neighbor 101.1.1.1
remote-as 100
address-family ipv4 unicast
  route-policy pass-all in
  route-policy pass-all out
!
!
router pim vrf default address-family ipv4
  rp-address 2.2.2.2
  interface Loopback0
    !
  interface GigabitEthernet0/0/0
    !
  interface GigabitEthernet0/0/3
    !
!
end

CE3:
For information about configuring the CE router, using Cisco IOS software, see the appropriate Cisco IOS software configuration documentation.

interface Loopback0
  ipv4 address 122.122.122.122 255.255.255.255
!

interface GigabitEthernet0/1/3/0
  ipv4 address 22.1.1.1 255.255.255.0
!

interface GigabitEthernet0/2/3/0
  ipv4 address 122.1.1.2 255.255.255.0

multicast-routing
  address-family ipv4
    interface all enable
    !
    !
  !
  route-policy pass-all
    pass
    end-policy
  !
router bgp 500
  bgp router-id 122.122.122.122
  address-family ipv4 unicast
    redistribute connected
    !
  neighbor 122.1.1.1
    remote-as 100
    address-family ipv4 unicast
      route-policy pass-all in
      route-policy pass-all out
    !
    !
  router pim vrf default address-family ipv4
    rp-address 2.2.2.2
    interface Loopback0
      !
    interface GigabitEthernet0/1/3/0
      !
Configuring Multitopology Routing: Example

The following example shows the configuration required to enable a dual multicast topology. The two topologies defined are named BLUE and GREEN. Each contains one interface. IS-IS is configured so that each interface is only in the IS-IS topology, and the interfaces themselves are configured so that their connected and local routes are placed only within the appropriate routing tables.

The routing policy was configured to select which topology should be used based on the source address of the multicast flow.

```
! interface GigabitEthernet0/1/0/0
 address-family ipv4 multicast topology BLUE
!
interface GigabitEthernet0/1/0/1
 address-family ipv4 multicast topology GREEN
!
router isis 1
 net 00.0000.0000.0001.00
interface GigabitEthernet0/1/0/0
 address-family ipv4 multicast topology BLUE
interface GigabitEthernet0/1/0/1
 address-family ipv4 multicast topology GREEN
!
route-policy mtp1
 if destination in (230.5.1.2) then
   if source in (10.10.10.10) then
     set rpf-topology ipv4 multicast topology BLUE
   else
     set rpf-topology ipv4 multicast topology GREEN
   endif
 endif
end-policy
!
router pim
 address-family ipv4
 rpf topology route-policy mtp1
!
!
multicast-routing
 address-family ipv4
 interface all enable
!
!
Examples 1 and 2 illustrate routing policies that you can use in configuring PIM RPF topologies:

**Example 1**

```
route-policy mtp1
 if destination in (225.0.0.1, 225.0.0.11) then
   set rpf-topology ipv4 multicast topology t201
 elseif destination in (225.0.0.2, 225.0.0.12) then
   set rpf-topology ipv4 multicast topology t202
endif
```

Example 1

```
set rpf-topology ipv4 multicast topology t202
elseif destination in (225.0.0.3, 225.0.0.13) then
    pass
endif
end-policy
```

Example 2

```
route-policy mtp2
    if destination in (225.0.0.8) then
        set rpf-topology ipv4 multicast topology t208
    elseif destination in (225.0.0.9) then
        set rpf-topology ipv4 multicast topology t209
    elseif destination in (225.0.0.10) then
        set rpf-topology ipv4 multicast topology t210
    else
        drop
    endif
end-policy
```

Configuring MVPN Extranet Routing: Example

These examples describe two ways to configure MVPN extranet routing:

- Configuring the Source MVRF on the Receiver PE Router: Example, page MCC-85
- Configuring the Receiver MVRF on the Source PE Router: Example, page MCC-88

For the full set of configuration tasks, see Configuring MVPN Extranet Routing, page MCC-52.

Configuring the Source MVRF on the Receiver PE Router: Example

The following examples show how to configure MVPN extranet routing by specifying the source MVRF on the receiver PE router.

You must configure both the source PE router and the receiver PE router.

Configure the Source PE Router Using Route Targets

```
interface Loopback5
    ipv4 address 201.5.5.201 255.255.255.255

interface Loopback22
    vrf provider-vrf
    ipv4 address 201.22.22.201 255.255.255.255

interface GigabitEthernet0/6/0/0
    vrf provider-vrf
    ipv4 address 10.10.10.1 255.255.0.0

vrf provider-vrf
    address-family ipv4 unicast
    import route-target 1100:1

export route-target 1100:1
```

router bgp 1
  regular BGP MVPN config
vrf provider-vrf
  rd 1100:1
  address-family ipv4 unicast
  redistribute connected

multicast-routing
vrf provider-vrf address-family ipv4
  mdt data 226.1.4.0/24 threshold 3
  log-traps
  mdt default ipv4 226.0.0.4
  rate-per-route
  interface all enable
  accounting per-prefix

multicast-routing
vrf receiver-vrf address-family ipv4
  nsf
  mdt source Loopback5
  interface all enable

router pim vrf provider-vrf address-family ipv4
  rp-address 201.22.22.201

Configure the Receiver PE Router Using Route Targets

interface Loopback5
  ipv4 address 202.5.5.202 255.255.255.255

interface GigabitEthernet0/3/0/2
  vrf receiver-vrf
  ipv4 address 20.20.20.1 255.255.0.0

vrf provider-vrf
  address-family ipv4 unicast
  import route-target
  1100:1
  export route-target
  1100:1

vrf receiver-vrf
  address-family ipv4 unicast
  import route-target
  1101:1
  import route-target
  1101:1

multicast-routing
vrf provider-vrf address-family ipv4
  log-traps
  mdt default ipv4 226.0.0.4
  rate-per-route
  interface all enable
accounting per-prefix
!
vrf receiver_vrf address-family ipv4
log-traps
mdt default ipv4 226.0.0.5
rate-per-route
interface all enable
accounting per-prefix
!
address-family ipv4
nsf
mdt source Loopback5
interface all enable
!
router pim vrf provider-vrf address-family ipv4
  rp-address 201.22.22.201
!
router pim vrf receiver_vrf address-family ipv4
  rp-address 201.22.22.201
!
router bgp 1
  regular BGP MVPN config
  vrf provider-vrf
    rd 1100:1
    address-family ipv4 unicast
    redistribute connected
  
  vrf receiver_vrf
    rd 1101:1
    address-family ipv4 unicast
    redistribute connected
!

Configuring RPL Policies in Receiver VRFS to Propagate Joins to a Source VRF: Example

In addition to configuring route targets, Routing Policy Language (RPL) policies can be configured in receiver VRFS on receiver PE routers to propagate joins to a specified source VRF. However, this configuration is optional.

The following configuration example shows a policy where the receiver VRF can pick either "provider_vrf_1" or "provider_vrf_2" to propagate PIM joins.

In this example, provider_vrf_1 is used for multicast streams in the range of from 227.0.0.0 to 227.255.255.255, while provider_vrf_2 is being used for streams in the range of from 228.0.0.0 to 228.255.255.255.

route-policy extranet_streams_from_provider_vrf
  if destination in (227.0.0.0/32 ge 8 le 32) then
    set rpf-topology vrf provider_vrf_1
  elseif destination in (228.0.0.0/32 ge 8 le 32) then
    set rpf-topology vrf provider_vrf_2
  else
    pass
  endif
end-policy
!
router pim vrf receiver_vrf address-family ipv4
  rpf topology route-policy extranet_streams_from_provider_vrf
!
Configuring the Receiver MVRF on the Source PE Router: Example

The following examples show how to configure MVPN extranet routing by specifying the receiver MVRF on the source PE router.

Note You must configure both the source PE router and the receiver PE router.

**Configure the Source PE Router Using Route Targets**

```
interface Loopback5
  ipv4 address 202.5.5.202 255.255.255.255
!
interface GigabitEthernet0/3/0/2
  vrf provider-vrf
  ipv4 address 20.20.20.1 255.255.0.0
!
  vrf provider-vrf
  address-family ipv4 unicast
  import route-target
  1100:1
  !
  export route-target
  1100:1
  !

  vrf receiver-vrf
  address-family ipv4 unicast
  import route-target
  1100:1
  1101:1
  !
  export route-target
  1101:1
  !

  router bgp 1
    regular BGP MVPN config
    vrf provider-vrf
    rd 1100:1
    address-family ipv4 unicast
    redistribute connected
    !
    vrf receiver-vrf
    rd 1101:1
    address-family ipv4 unicast
    redistribute connected
    !

  multicast-routing
    vrf provider-vrf address-family ipv4
    log-traps
    mdt default ipv4 226.0.0.4
    rate-per-route
    interface all enable
    accounting per-prefix
    !
```
vrf receiver_vrf address-family ipv4
log-traps
mdt default ipv4 226.0.0.5
rate-per-route
interface all enable
accounting per-prefix
!
address-family ipv4
nsf
mdt source Loopback5
interface all enable
!
router pim vrf provider-vrf address-family ipv4
rp-address 201.22.22.201
!
router pim vrf receiver_vrf address-family ipv4
rp-address 201.22.22.201
!

Configure the Receiver PE Router Using Route Targets
interface Loopback5
  ipv4 address 201.5.5.201 255.255.255.255
!
interface Loopback22
  vrf receiver_vrf
    ipv4 address 201.22.22.201 255.255.255.255
!
interface GigabitEthernet0/6/0/0
  vrf receiver_vrf
    ipv4 address 10.10.10.1 255.255.0.0
!

vrf receiver_vrf
  address-family ipv4 unicast
  import route-target
    1100:1
    1101:1
  !
  export route-target
    1101:1
  !

router bgp 1
  regular BGP MVPN config
  vrf receiver_vrf
    rd 1101:1
    address-family ipv4 unicast
    redistribute connected
    !

  multicast-routing
    vrf receiver_vrf address-family ipv4
    log-traps
    mdt default ipv4 226.0.0.5
    rate-per-route
    interface all enable
    accounting per-prefix
    !
    address-family ipv4
    nsf
    mdt source Loopback5
interface all enable
!
router pim vrf receiver_vrf address-family ipv4
  rp-address 201.22.22.201
!

Configuring RPL Policies in Receiver VRFs on Source PE Routers to Propagate Joins to a Source VRF: Example

In addition to configuring route targets, RPL policies can be configured in receiver VRFs on a source PE router to propagate joins to a specified source VRF. However, this configuration is optional.

The configuration below shows a policy in which the receiver VRF can select either “provider_vrf_1” or “provider_vrf_2” to propagate PIM joins. Provider_vrf_1 will be selected if the rendezvous point (RP) for a multicast stream is 201.22.22.201, while provider_vrf_2 will be selected if the RP for a multicast stream is 202.22.22.201.

As an alternative, you can configure a multicast group-based policy as shown in the “Configuring RPL Policies in Receiver VRFs to Propagate Joins to a Source VRF: Example” section on page MCC-87.

route-policy extranet_streams_from_provider_rp
  if source in (201.22.22.201) then
    set rpf-topology vrf provider_vrf_1
  else if source in (202.22.22.201) then
    set rpf-topology vrf provider_vrf_2
  else
    pass
  endif
end-policy
!
router pim vrf receiver_vrf address-family ipv4
  rp topology route-policy extranet_streams_from_provider_rp
  rp-address 201.22.22.201 grange_227
  rp-address 202.22.22.201 grange_228
!

Configuring Multicast Hub and Spoke Topology: Example

These examples describe two ways to configure Multicast Hub and Spoke:

- Hub and Spoke Non-Turnaround Configuration: Example, page MCC-91
- Hub and Spoke with Turnaround: Example, page MCC-100

Figure 10 Example for Multicast Hub and Spoke Topology

CE1——PE1——PE3——CE3

CE1, PE1, and PE3 are all on Cisco IOS XR Software, CE3 has Cisco IOS Software in order to configure autorp on VRF interface. For information about configuring the CE router, using Cisco IOS software, see the appropriate Cisco IOS software documentation.
Hub and Spoke Non-Turnaround Configuration: Example

A1-Spoke-3

No turnaround case with bsr and autorp relay

PE1:

vrf A1-Hub-1
address-family ipv4 unicast
import route-target

1000:10
1001:10
!
export route-target
1000:10
!
!
!
vrf A1-Hub-Tunnel
address-family ipv4 unicast
import route-target
1000:10
!
!
!
!
vrf A1-Spoke-Tunnel
address-family ipv4 unicast
import route-target
1001:10
!
!
!
!
router pim
vrf A1-Hub-1
address-family ipv4
rpf topology route-policy A1-Hub-Policy
bsr relay vrf A1-Hub-Tunnel
bsr candidate-bsr 201.10.10.201 hash-mask-len 30 priority 4
bsr candidate-rp 201.10.10.201 group-list A1_PE1_RP_grange priority 4 interval 60
auto-rp relay vrf A1-Hub-Tunnel
!
!
!
router pim
vrf A1-Hub-Tunnel
  address-family ipv4
  !
  !
  !
multicast-routing
vrf A1-Hub-1
  address-family ipv4
  log-traps
  multipath
  rate-per-route
  interface all enable
  accounting per-prefix
  !
  !
  !
multicast-routing
vrf A1-Hub-Tunnel
  address-family ipv4
  mdt data 226.202.1.0/24 threshold 10
  log-traps
  mdt default ipv4 226.202.0.0
  rate-per-route
  accounting per-prefix
  !
multicast-routing
vrf A1-Spoke-Tunnel
  address-family ipv4
    mdt mtu 2000
    mdt data 226.202.2.0/24 threshold 5
    log-traps
    mdt default ipv4 226.202.0.1
    rate-per-route
    accounting per-prefix
!
!
!
router bgp 1
  vrf A1-Hub-1
    rd 1000:1
    address-family ipv4 unicast
      route-target download
      redistribute connected
      redistribute eigrp 20 match internal external metric 1000
!
!
!
router bgp 1
  vrf A1-Hub-Tunnel
    rd 1002:1
    address-family ipv4 unicast
      redistribute connected
!
!
!
router bgp 1
vrf A1-Spoke-Tunnel
  rd 1002:2
  address-family ipv4 unicast
    redistribute connected
  !
  !
  !
  route-policy A1-Hub-Policy
    if extcommunity rt matches-any (1000:10) then
      set rpf-topology vrf A1-Hub-Tunnel
    elseif extcommunity rt matches-any (1001:10) then
      set rpf-topology vrf A1-Spoke-Tunnel
    else
      pass
    endif
  end-policy
  !
  route-policy A1-Spoke-Policy
    if extcommunity rt matches-any (1000:10) then
      set rpf-topology vrf A1-Hub-Tunnel
    else
      pass
    endif
  end-policy
  !

PE3:
  vrf A1-Hub-4
  address-family ipv4 unicast
  import route-target
    1000:10
    1001:10
  !
  export route-target
vrf A1-Spoke-2
address-family ipv4 unicast
import route-target
  1000:10

export route-target
  1001:10

vrf A1-Spoke-Tunnel
address-family ipv4 unicast
import route-target
  1000:10

vrf A1-Hub-Tunnel
address-family ipv4 unicast
import route-target
  1001:10

router pim
vrf A1-Hub-4
address-family ipv4
  rpf topology route-policy A1-Hub-Policy
  bsr relay vrf A1-Hub-Tunnel listen
  auto-rp relay vrf A1-Hub-Tunnel
```
! router pim
vrf A1-Spoke-2
  address-family ipv4
    rpf topology route-policy A1-Spoke-Policy
    bsr relay vrf A1-Hub-Tunnel listen
    auto-rp relay vrf A1-Hub-4
!
!
!
multicast-routing
vrf A1-Hub-4
  address-family ipv4
    log-traps
    rate-per-route
    interface all enable
    accounting per-prefix
!
!
!
multicast-routing
vrf A1-Spoke-2
  address-family ipv4
    log-traps
    rate-per-route
    interface all enable
    accounting per-prefix
!
!
!
multicast-routing
vrf A1-Hub-Tunnel
```
address-family ipv4
  mdt data 226.202.1.0/24 threshold 10
  log-traps
  mdt default ipv4 226.202.0.0
  rate-per-route
  accounting per-prefix
!
!
!
multicast-routing
vrf A1-Spoke-Tunnel
  address-family ipv4
  mdt data 226.202.2.0/24 threshold 5
  log-traps
  mdt default ipv4 226.202.0.1
  rate-per-route
  accounting per-prefix
!
!
!
router bgp 1
  vrf A1-Hub-4
    rd 1000:4
    address-family ipv4 unicast
      route-target download
      redistribute connected
      redistribute eigrp 4 match internal external metric 1000
!
!
!
router bgp 1
  vrf A1-Spoke-2
    rd 1001:2
address-family ipv4 unicast
route-target download
redistribute connected
redistribute eigrp 6 match internal external metric 1000
!
!
router bgp 1
vrf A1-Hub-Tunnel
rd 1002:1
address-family ipv4 unicast
redistribute connected
!
!
!
router bgp 1
vrf A1-Spoke-Tunnel
rd 1002:2
address-family ipv4 unicast
redistribute connected
!
!
!
route-policy A1-Hub-Policy
if extcommunity rt matches-any (1000:10) then
    set rpf-topology vrf A1-Hub-Tunnel
elsif extcommunity rt matches-any (1001:10) then
    set rpf-topology vrf A1-Spoke-Tunnel
else
    pass
endif
end-policy
!
route-policy A1-Spoke-Policy
if extcommunity rt matches-any (1000:10) then
    set rpf-topology vrf A1-Hub-Tunnel
else
    pass
endif
end-policy
!

CE1:

vrf A1-Hub-1
    address-family ipv4 unicast
    import route-target
    1000:10
    1001:10
    !
    export route-target
    1000:10
    !
    !
    !
    ! multicast-routing
    vrf A1-Hub-1
    address-family ipv4
    log-traps
    rate-per-route
    interface all enable
    accounting per-prefix
    !
    !
    !
No router pim configuration required
CE3: Where autorp is configured (this is an Cisco IOS Software example, because auto-rp on vrf interface is not supported in Cisco IOS XR Software)

ip vrf A1-Hub-4
rd 1000:4
route-target export 1000:10
route-target import 1000:10
route-target import 1001:10
!
ip vrf A1-Spoke-2
rd 1001:2
route-target export 1001:10
route-target import 1000:10
!
ip multicast-routing vrf A1-Hub-4
ip multicast-routing vrf A1-Spoke-2

interface Loopback10
ip vrf forwarding A1-Hub-4
ip address 103.10.10.103 255.255.255.255
ip pim sparse-mode
!
ip pim vrf A1-Hub-4 autorp listener
ip pim vrf A1-Hub-4 send-rp-announce Loopback10 scope 32
ip pim vrf A1-Hub-4 send-rp-discovery Loopback10 scope 32

Hub and Spoke with Turnaround: Example

Multicast turnaround mandates a 2-interface connection to the hub site
To configure a CE as a turnaround router, it is connected to its respective PE through two interfaces and each interface is placed in a separate hub site vrf called hub-x-in vrf and hub-x-out vrf. Hub-x-in vrf carries joins that come from the receiver spoke site through the Hub Tunnel and hub-x-out vrf will carry the same joins towards the source spoke site through the Spoke Tunnel without violating the four basic rules below. The source spoke sends traffic to the spoke tunnel to hub-x-out which is turned around to the hub-tunnel on the hub-x-in interface.

1. Hub sites sends traffic only to MDTHub.
2. Spoke sites sends traffic only to MDTspoke.
3. Hub sites receives traffic from both tunnels.
4. Spoke sites receive traffic only from MDTHub.

A2-Spoke-1  A2-Hub-2
A2-Spoke-2  A2-Hub-3in
              A2-Hub-2out
              A2-Spoke-3 (spoke has auto-rp)

Figure 11  Example for Multicast Hub and Spoke Topology with Turaround

CE1——— PE1 ———————————— PE2——— CE2

Routes exported by hub sites are imported by hub sites and spoke sites. Routes exported by spoke sites are imported by both **hub-x-out** and **hub-x-in** and hub site exports spoke routes back into the core by hub VRF route targets. This causes routes originated from one spoke site to be learned by all other spoke sites but with the next hop of **hub-x-out**. For example, Spoke2 will see the RPF for Spoke1 reachable with next hop of **A2-Hub-3in**. This is the fundamental difference in leaking of routes which helps in achieving turnaround of multicast traffic.

**PE1:**

vrf A2-Spoke-1

address-family ipv4 unicast

import route-target

4000:1
4000:2
4000:3
4000:4

! export route-target

4001:1

!
!
!
!

vrf A2-Spoke-2

address-family ipv4 unicast

import route-target

4000:1
4000:2
4000:3
4000:4

! export route-target
  4001:2
  !
  !

PE2:

vrf A2-Hub-2
  address-family ipv4 unicast
    import route-target
    4000:1
    4000:2
    4000:3
    4000:4
    4001:1
    4001:2
    4001:3
    4001:4
    ! export route-target
    4000:2
    !
    !
    !

  vrf A2-Hub-3out
    address-family ipv4 unicast
    import route-target
    4000:1
4000:2
4000:3
4000:4

4001:1 --------à exports the spoke routes into CE2 into vrf default
4001:2 --------à exports the spoke routes into CE2 into vrf default
4001:3 --------à exports the spoke routes into CE2 into vrf default
4001:4 --------à exports the spoke routes into CE2 into vrf default

export route-target
4000:4

vrf A2-Hub-3in
address-family ipv4 unicast
import route-target
4000:1
4000:2
4000:3
4000:4

export route-target
4000:3--------à selected spoke routes (in the prefix-set below) can be re-exported with hub route target so other spokes can reach them via A2-Hub-3in

prefix-set A2-Spoke-family
112.31.1.0/24,
112.32.1.0/24,
152.31.1.0/24,
132.30.1.0/24,
102.9.9.102/32,
103.31.31.103/32,
183.31.1.0/24,
183.32.1.0/24
end-set
!

route-policy A2-Spoke-family
  if destination in A2-Spoke-family then
    pass
  else
    drop
  endif
end-policy
!

router bgp 1
vrf A2-Hub-3in
  rd 4000:3
  address-family ipv4 unicast
    route-target download
    redistribute connected
  !
neighbor 113.113.114.9
  remote-as 12
  address-family ipv4 unicast
    route-policy A2-Spoke-family in
    route-policy pass-all out
  !
  !
  !
router bgp 1
  vrf A2-Hub-3out
  rd 4000:4
  address-family ipv4 unicast
   route-target download
   redistribute connected
  !
  !
  !
  router bgp 1
  vrf A2-Hub-2
  rd 4000:2
  address-family ipv4 unicast
   route-target download
   redistribute connected
   redistribute eigrp 20 match internal external metric 1000
  !
  !
  !
multicast-routing
  vrf A2-Hub-2
  address-family ipv4
   log-traps
   rate-per-route
   interface all enable
   accounting per-prefix
  !
  !
  !
multicast-routing
  vrf A2-Hub-3in
  address-family ipv4
log-traps
rate-per-route
interface all enable
accounting per-prefix
!
!
!

multicast-routing
vrf A2-Hub-3out
address-family ipv4
log-traps
rate-per-route
interface all enable
accounting per-prefix
!
!
!

router pim
vrf A2-Hub-2
address-family ipv4
rpf topology route-policy A2-Hub-Policy
bsr relay vrf A2-Spoke-3 listen
auto-rp relay vrf A2-Hub-Tunnel
!
!
!

router pim
vrf A2-Hub-3in
address-family ipv4
rpf topology route-policy A2-Hub-Policy
!
!
!

router pim
vrf A2-Hub-3out
address-family ipv4
rpf topology route-policy A2-Hub-Policy
!
!
! route-policy A2-Hub-Policy
if extcommunity rt matches-any (4000:1, 4000:2, 4000:3, 4000:4) then
set rpf-topology vrf A2-Hub-Tunnel
elseif extcommunity rt matches-any (4001:1, 4001:2, 4001:3, 4001:4) then
set rpf-topology vrf A2-Spoke-Tunnel
else
pass
endif
end-policy
!

Any CE-PE protocol can be used. In this example, A2-Hub-3out exports all the hub and spoke routes to CE2 through EIGRP.

A2-Hub-3in uses route policy A2-Spoke-family to re-import selected spoke routes into PE2 through BGP.

```
router eigrp 20
vrf A2-Hub-3out
address-family ipv4
default-metric 1000 1 255 1 1500
autonomous-system 20
redistribute bgp 1
interface GigabitEthernet0/1/0/1.13
hold-time 60
```

```
CE2:
Here A2-Hub-3in and A2-Hub-3out interfaces are in vrf default and not in a hub site vrf.

interface GigabitEthernet0/12/1/0.12
description To PE2 or vrf A2-Hub-3in
ipv4 address 113.113.114.9 255.255.255.252
dot1q vlan 3001
!
interface GigabitEthernet0/12/1/0.13
description To PE2 or vrf A2-Hub-3out
ipv4 address 113.113.114.13 255.255.255.252
dot1q vlan 3002
!
router bgp 12
nsr
bgp graceful-restart

address-family ipv4 unicast
redistribute connected
redistribute eigrp 20
!
neighbor 113.113.114.10 --à this is the A2-Hub-3in neighbor on PE2.
remote-as 1
```
address-family ipv4 unicast
route-policy pass-all in
route-policy pass-all out
!
!

Additional References

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multicast command reference document</td>
<td>Cisco IOS XR Multicast Command Reference for the CiscoCRS Router</td>
</tr>
<tr>
<td>Getting started material</td>
<td>Cisco IOS XR Aggregation Services Router Getting Started Guide for the CiscoCRS Router</td>
</tr>
<tr>
<td>Modular quality of service command reference document</td>
<td>Cisco IOS XR Aggregation Services Router Modular Quality of Service Command Reference for the CiscoCRS Router</td>
</tr>
<tr>
<td>Routing command reference and configuration documents</td>
<td>Cisco IOS XR Routing Command Reference and Cisco IOS XR Routing Configuration Guide for CiscoCRS Router</td>
</tr>
<tr>
<td>Information about user groups and task IDs</td>
<td>Configuring AAA Services on Cisco IOS XR Software module of CiscoCRS Router System Security Configuration Guide</td>
</tr>
</tbody>
</table>
Standards

<table>
<thead>
<tr>
<th>Standards</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>draft-ietf-l3vpn-rfc2547bis</td>
<td>BGP/MPLS IP VPNs</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIBs</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>—</td>
<td>To locate and download MIBs using Cisco IOS XR software, use the Cisco MIB Locator found at the following URL and choose a platform under the Cisco Access Products menu: <a href="http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a></td>
</tr>
</tbody>
</table>

RFCs

<table>
<thead>
<tr>
<th>RFCs</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 2385</td>
<td>Protection of BGP Sessions via the TCP MD5 Signature Option</td>
</tr>
<tr>
<td>RFC 2547</td>
<td>BGP/MPLS VPNs</td>
</tr>
<tr>
<td>RFC 2710</td>
<td>Multicast Listener Discovery (MLD) for IPv6</td>
</tr>
<tr>
<td>RFC 3376</td>
<td>Internet Group Management Protocol, Version 3</td>
</tr>
<tr>
<td>RFC 3446</td>
<td>Anycast Rendezvous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)</td>
</tr>
<tr>
<td>RFC 3618</td>
<td>Multicast Source Discovery Protocol (MSDP)</td>
</tr>
<tr>
<td>RFC 3810</td>
<td>Multicast Listener Discovery Version 2 (MLDv2) for IPv6</td>
</tr>
<tr>
<td>RFC4875</td>
<td>Extensions to Resource Reservation Protocol - Traffic Engineering (RSVP-TE) for Point-to-Multipoint TE Label-Switched Paths (LSPs)</td>
</tr>
<tr>
<td>RFC 4364</td>
<td>BGP/MPLS IP Virtual Private Networks</td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.</td>
<td><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></td>
</tr>
</tbody>
</table>